Cisco Wireless Controller Command Reference, Release 8.5

First Published: 2017-07-21

Last Modified: 2021-02-12

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

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

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

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

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

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

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

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

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

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

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

© 2017–2021 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface liii

Audience liii

Document Conventions liii

Related Documentation lvi

Communications, Services, and Additional Information lvi

Cisco Bug Search Tool lvi

Documentation Feedback lvi

PART I

Using the Command-Line Interface 57

CHAPTER 1

Using the Command-Line Interface 1

CLI Command Keyboard Shortcuts 2

Using the Interactive Help Feature 4

Using the help Command 4

Using the ? command 5

Using the partial? command 5

Using the partial command<tab> 6

Using the command ? 6

command keyword ? 6

PART II

Clear Commands 7

CHAPTER 2

Clear Commands: a to l 9

clear advanced 10

clear acl counters 11

clear ap config 12

clear ap eventlog 13
clear ap join stats 14
clear arp 15
clear ap tsm 16
clear atf 17
clear avc statistics 18
clear client tsm 20
clear config 21
clear ext-webauth-url 22
clear location rfid 23
clear location statistics rfid 24
clear locp statistics 25
clear login-banner 26
clear lwapp private-config 27

CHAPTER 3 **Clear Commands: m to z** 29
clear mdns service-database 30
clear nmsp statistics 31
clear radius acct statistics 32
clear tacacs auth statistics 33
clear redirect-url 34
clear stats ap wlan 35
clear stats local-auth 36
clear stats mobility 37
clear stats port 38
clear stats radius 39
clear stats smart-lic 40
clear stats switch 41
clear stats tacacs 42
clear transfer 43
clear traplog 44
clear urlacl-counters 45
clear webimage 46
clear webmessage 47

clear webtitle 48

PART III Config Commands 49

CHAPTER 4 Config Commands: 802.11 51

config 802.11-abgn 54
config 802.11a 11acsupport 55
config 802.11-a antenna extAntGain 56
config 802.11-a channel ap 57
config 802.11-a txpower ap 58
config 802.11 antenna diversity 59
config 802.11 antenna extAntGain 60
config 802.11 antenna mode 61
config 802.11 antenna selection 62
config 802.11b 11gSupport 63
config 802.11b preamble 64
config 802.11h channelswitch 65
config 802.11h powerconstraint 66
config 802.11h setchannel 67
config 802.11 11nsupport 68
config 802.11 11nsupport a-mpdu tx priority 69
config 802.11 11nsupport a-mpdu tx scheduler 71
config 802.11 11nsupport antenna 72
config 802.11 11nsupport guard-interval 73
config 802.11 11nsupport mcs tx 74
config 802.11 11nsupport rifs 76
config 802.11 antenna diversity 77
config 802.11 antenna extAntGain 78
config 802.11 antenna mode 79
config 802.11 antenna selection 80
config 802.11 channel 81
config 802.11 channel ap 83
config 802.11 chan_width 84
config 802.11 rx-sop threshold 86

config 802.11 txPower 87
config 802.11 beamforming 89
config 802.11h channelswitch 90
config 802.11h powerconstraint 91
config 802.11h setchannel 92
config 802.11h smart dfs 93
config 802.11 11nsupport 94
config 802.11 11nsupport a-mpdu tx priority 95
config 802.11 11nsupport a-mpdu tx scheduler 97
config 802.11 11nsupport antenna 98
config 802.11 11nsupport guard-interval 99
config 802.11 11nsupport mcs tx 100
config 802.11 11nsupport rifs 102
config 802.11 beacon period 103
config 802.11 cac defaults 104
config 802.11 cac video acm 106
config 802.11 cac video cac-method 108
config 802.11 cac video load-based 110
config 802.11 cac video max-bandwidth 112
config 802.11 cac media-stream 114
config 802.11 cac multimedia 116
config 802.11 cac video roam-bandwidth 118
config 802.11 cac video sip 120
config 802.11 cac video tspec-inactivity-timeout 122
config 802.11 cac voice acm 123
config 802.11 cac voice max-bandwidth 124
config 802.11 cac voice roam-bandwidth 126
config 802.11 cac voice tspec-inactivity-timeout 128
config 802.11 cac voice load-based 130
config 802.11 cac voice max-calls 132
config 802.11 cac voice sip bandwidth 134
config 802.11 cac voice sip codec 136
config 802.11 cac voice stream-size 138
config 802.11 cleanair 140

config 802.11 cleanair device 142
config 802.11 cleanair alarm 144
config 802.11 disable 146
config 802.11 dtpc 147
config 802.11 enable 148
config 802.11 exp-bwreq 149
config 802.11 fragmentation 150
config 802.11 l2roam rf-params 151
config 802.11 max-clients 153
config 802.11 media-stream multicast-direct 154
config 802.11 media-stream video-redirect 156
config 802.11 multicast data-rate 157
config 802.11 rate 158
config 802.11 rssi-check 159
config 802.11 rssi-threshold 160
config 802.11 tsm 161
config 802.11b preamble 162

CHAPTER 5 **Config Commands: a to i** 163

config aaa auth 171
config aaa auth mgmt 172
config acl apply 173
config acl counter 174
config acl create 175
config acl cpu 176
config acl delete 177
config acl layer2 178
config acl rule 180
config acl url-acl 182
config acl url-acl apply 183
config acl url-acl external-server-ip 184
config acl url-acl list-type 185
config acl url-domain 186
config advanced 802.11 7920VSIEConfig 187

config advanced 802.11 channel add 188
config advanced 802.11 channel cleanair-event 189
config advanced 802.11 channel dca anchor-time 190
config advanced 802.11 channel dca chan-width-11n 191
config advanced 802.11 channel dca interval 192
config advanced 802.11 channel dca min-metric 193
config advanced 802.11 channel dca sensitivity 194
config advanced 802.11 channel foreign 196
config advanced 802.11 channel load 197
config advanced 802.11 channel noise 198
config advanced 802.11 channel outdoor-ap-dca 199
config advanced 802.11 channel pda-prop 200
config advanced 802.11 channel update 201
config advanced 802.11 coverage 202
config advanced 802.11 coverage exception global 203
config advanced 802.11 coverage fail-rate 204
config advanced 802.11 coverage level global 205
config advanced 802.11 coverage packet-count 206
config advanced 802.11 coverage rssi-threshold 207
config advanced 802.11 edca-parameters 209
config advanced 802.11 factory 211
config advanced 802.11 group-member 212
config advanced 802.11 group-mode 213
config advanced 802.11 logging channel 214
config advanced 802.11 logging coverage 215
config advanced 802.11 logging foreign 216
config advanced 802.11 logging load 217
config advanced 802.11 logging noise 218
config advanced 802.11 logging performance 219
config advanced 802.11 logging txpower 220
config advanced 802.11 monitor channel-list 221
config advanced 802.11 monitor load 222
config advanced 802.11 monitor measurement 223
config advanced 802.11 monitor mode 224

config advanced 802.11 monitor ndp-type 225
config advanced 802.11 monitor timeout-factor 226
config advanced 802.11 optimized roaming 227
config advanced 802.11 packet 228
config advanced 802.11 profile clients 230
config advanced 802.11 profile customize 231
config advanced 802.11 profile foreign 232
config advanced 802.11 profile noise 233
config advanced 802.11 profile throughput 234
config advanced 802.11 profile utilization 235
config advanced 802.11 receiver 236
config advanced 802.11 reporting measurement 237
config advanced 802.11 tpc-version 238
config advanced 802.11 tpcv1-thresh 239
config advanced 802.11 tpcv2-intense 240
config advanced 802.11 tpcv2-per-chan 241
config advanced 802.11 tpcv2-thresh 242
config advanced 802.11 txpower-update 243
config advanced eap 244
config advanced fra service-priority 246
config advanced fra client-aware client-select 247
config advanced fra client-aware client-reset 248
config advanced hyperlocation 249
config advanced hyperlocation apgroup 250
config advanced hyperlocation ble-beacon 251
config advanced hyperlocation ble-beacon beacon-id 252
config advanced hotspot 253
config advanced timers auth-timeout 254
config advanced timers eap-timeout 255
config advanced timers eap-identity-request-delay 256
config advanced timers 257
config advanced fastpath fastcache 260
config advanced fastpath pkt-capture 261
config advanced sip-preferred-call-no 262

config advanced sip-snooping-ports 263
config advanced backup-controller primary 264
config advanced backup-controller secondary 265
config advanced client-handoff 266
config advanced dot11-padding 267
config advanced assoc-limit 268
config advanced max-1x-sessions 269
config advanced rate 270
config advanced probe filter 271
config advanced probe limit 272
config advanced timers 273
config ap 802.1Xuser 276
config ap 802.1Xuser delete 277
config ap 802.1Xuser disable 278
config advanced dot11-padding 279
config ap 280
config ap aid-audit 281
config ap antenna band-mode 282
config ap atf 802.11 283
config ap atf 802.11 client-access airtime-allocation 284
config ap atf 802.11 policy 285
config ap autoconvert 286
config ap bhrate 287
config ap bridgegroupname 288
config ap bridging 289
config ap cdp 290
config ap cert-expiry-ignore 292
config ap core-dump 293
config ap crash-file clear-all 294
config ap crash-file delete 295
config ap crash-file get-crash-file 296
config ap crash-file get-radio-core-dump 297
config ap dhcp release-override 298
config ap dtls-cipher-suite 299

config ap dtls-version 300
config ap ethernet duplex 301
config ap ethernet tag 302
config ap autoconvert 303
config ap flexconnect central-dhcp 304
config ap flexconnect local-split 305
config ap flexconnect module-vlan 306
config ap flexconnect policy 307
config ap flexconnect radius auth set 308
config ap flexconnect vlan 309
config ap flexconnect vlan add 310
config ap flexconnect vlan native 311
config ap flexconnect vlan wlan 312
config ap flexconnect web-auth 313
config ap flexconnect web-policy acl 314
config ap flexconnect wlan 315
config ap group-name 316
config ap hotspot 317
config ap image predownload 324
config ap image swap 325
config ap ipsla 326
config ap led-state 327
config ap link-encryption 328
config ap link-latency 329
config ap location 330
config ap logging syslog level 331
config ap logging syslog facility 332
config ap max-count 334
config ap mgmtuser add 335
config ap mgmtuser delete 336
config ap mode 337
config ap module3g 339
config ap monitor-mode 340
config ap name 341

config ap packet-dump 342
config ap port 345
config ap power injector 346
config ap power pre-standard 347
config ap preferred-mode 348
config ap primary-base 349
config ap priority 350
config ap reporting-period 351
config ap reset 352
config ap retransmit interval 353
config ap retransmit count 354
config ap role 355
config ap rst-button 356
config ap secondary-base 357
config ap sniff 358
config ap ssh 359
config ap static-ip 360
config ap stats-timer 362
config ap syslog host global 363
config ap syslog host specific 364
config ap tcp-mss-adjust 365
config ap telnet 366
config ap tertiary-base 367
config ap tftp-downgrade 368
config ap username 369
config ap venue 370
config ap wlan 374
config atf 802.11 375
config atf policy 376
config auth-list add 377
config auth-list ap-policy 378
config auth-list delete 379
config avc profile create 380
config avc profile delete 381

config avc profile rule 382
config band-select cycle-count 384
config band-select cycle-threshold 385
config band-select expire 386
config band-select client-rssi 387
config boot 388
config call-home contact email address 389
config call-home events 390
config call-home http-proxy ipaddr 391
config call-home http-proxy ipaddr 0.0.0.0 392
config call-home profile 393
config call-home profile delete 394
config call-home profile status 395
config call-home reporting 396
config call-home tac-profile 397
config cdp 398
config certificate 399
config certificate lsc 400
config certificate ssc 402
config certificate use-device-certificate webadmin 403
config client ccx clear-reports 404
config client ccx clear-results 405
config client ccx default-gw-ping 406
config client ccx dhcp-test 407
config client ccx dns-ping 408
config client ccx dns-resolve 409
config client ccx get-client-capability 410
config client ccx get-manufacturer-info 411
config client ccx get-operating-parameters 412
config client ccx get-profiles 413
config client ccx log-request 414
config client ccx send-message 416
config client ccx stats-request 420
config client ccx test-abort 421

config client ccx test-association 422
config client ccx test-dot1x 423
config client ccx test-profile 424
config client deauthenticate 425
config client location-calibration 426
config client profiling delete 427
config cloud-services cmx 428
config cloud-services server url 429
config cloud-services server id-token 430
config coredump 431
config coredump ftp 432
config coredump username 433
config country 434
config cts 435
config cts ap 436
config cts inline-tag 437
config cts ap override 438
config cts device-id 439
config cts refresh 440
config cts sxp ap connection delete 441
config cts sxp ap connection peer 442
config cts sxp ap default password 443
config cts sxp ap listener 444
config cts sxp ap reconciliation period 445
config cts sxp ap retry period 446
config cts sxp ap speaker 447
config cts sxp 448
config cts sxp connection 449
config cts sxp default password 450
config cts sxp retry period 451
config cts sxp version 452
config cts sxp 453
config custom-web ext-webauth-mode 454
config custom-web ext-webauth-url 455

config custom-web ext-webserver 456
config custom-web logout-popup 457
config custom-web qrscan-bypass-opt 458
config custom-web radiusauth 459
config custom-web redirectUrl 460
config custom-web sleep-client 461
config custom-web webauth-type 462
config custom-web weblogo 463
config custom-web webmessage 464
config custom-web webtitle 465
config database size 466
config dhcp 467
config dhcp opt-82 format 469
config dhcp opt-82 remote-id 470
config dhcp proxy 471
config dhcp timeout 472
config dx 473
config exclusionlist 474
config fabric 475
config fabric vnid create name 476
config fabric control-plane enterprise-fabric 477
config fabric control-plane guest-fabric 478
config flexconnect [ipv6] acl 479
config flexconnect [ipv6] acl rule 480
config flexconnect [ipv6] acl url-domain 482
config flexconnect arp-caching 483
config flexconnect avc profile 484
config flexconnect fallback-radio-shut 485
config flexconnect group 486
config flexconnect group vlan 491
config flexconnect group group-name dhcp overridden-interface 492
config flexconnect group web-auth 493
config flexconnect group web-policy 494
config flexconnect join min-latency 495

config flexconnect office-extend 496
config flow 497
config guest-lan 498
config guest-lan custom-web ext-webauth-url 499
config guest-lan custom-web global disable 500
config guest-lan custom-web login_page 501
config guest-lan custom-web webauth-type 502
config guest-lan ingress-interface 503
config guest-lan interface 504
config guest-lan mobility anchor 505
config guest-lan nac 506
config guest-lan security 507
config interface 3g-vlan 508
config interface acl 509
config interface address 510
config interface address redundancy-management 512
config interface ap-manager 513
config interface create 514
config interface delete 515
config interface dhcp management 516
config interface dhcp 518
config interface dhcp dynamic-interface 519
config interface dhcp management option-6-opendns 520
config interface address 521
config interface group failure-detect 523
config interface group mdns-profile 524
config interface guest-lan 525
config interface hostname 526
config interface nasid 527
config interface nat-address 528
config interface port 529
config interface quarantine vlan 530
config interface url-acl 531
config interface vlan 532

config interface mdns-profile 533
config icons delete 535
config icons file-info 536
config ipv6 disable 537
config ipv6 enable 538
config ipv6 acl 539
config ipv6 capwap 541
config ipv6 interface 542
config ipv6 multicast 544
config ipv6 neighbor-binding 545
config ipv6 ns-mcast-fwd 547
config ipv6 ra-guard 548
config ipv6 route 549

CHAPTER 6 Config Commands: j to q 551
config known ap 557
config lag 558
config ldap 559
config local-auth active-timeout 561
config local-auth cipher-option 562
config local-auth eap-profile 563
config local-auth method fast 565
config local-auth user-credentials 567
config lync-sdn 568
config licensing 569
config license boot 570
config load-balancing 571
config location 573
config location info rogue 575
config logging buffered 576
config logging console 577
config logging debug 578
config logging fileinfo 579
config logging procinfo 580

config logging traceinfo 581
config logging syslog host 582
config logging syslog facility 585
config logging syslog facility client 587
config logging syslog facility ap 588
config logging syslog ipsec 589
config logging syslog ipsec profile 590
config logging syslog tls 591
config logging syslog level 592
config loginsession close 593
config macfilter 594
config macfilter description 595
config macfilter interface 596
config macfilter ip-address 597
config macfilter mac-delimiter 598
config macfilter radius-compat 599
config macfilter wlan-id 600
config mdns ap 601
config mdns profile 602
config mdns query interval 604
config mdns service 605
config mdns snooping 607
config mdns policy enable 608
config mdns policy service-group 609
config mdns policy service-group parameters 610
config mdns policy service-group user-name 611
config mdns policy service-group user-role 612
config media-stream multicast-direct 613
config media-stream message 614
config media-stream add 615
config media-stream admit 617
config media-stream deny 618
config media-stream delete 619
config memory monitor errors 620

config memory monitor leaks 621
config mesh alarm 623
config mesh astools 624
config mesh backhaul rate-adapt 625
config mesh backhaul slot 626
config mesh battery-state 627
config mesh client-access 628
config mesh ethernet-bridging allow-bpdu 629
config mesh ethernet-bridging vlan-transparent 630
config mesh full-sector-dfs 631
config mesh linkdata 632
config mesh linktest 634
config mesh lsc 637
config mesh lsc advanced 638
config mesh lsc advanced ap-provision 639
config mesh multicast 640
config mesh parent preferred 642
config mesh public-safety 643
config mesh radius-server 644
config mesh range 645
config mesh secondary-backhaul 646
config mesh security 647
config mesh slot-bias 649
config mgmtuser add 650
config mgmtuser delete 651
config mgmtuser description 652
config mgmtuser password 653
config mgmtuser telnet 654
config mgmtuser termination-interval 655
config mobility dscp 656
config mobility encryption tunnel 657
config mobility group anchor 658
config mobility group domain 659
config mobility group keepalive count 660

config mobility group keepalive interval 661
config mobility group member 662
config mobility group multicast-address 664
config mobility multicast-mode 665
config mobility new-architecture 666
config mobility oracle 667
config mobility secure-mode 668
config mobility statistics reset 669
config netuser add 670
config netuser delete 672
config netuser description 673
config netuser guest-lan-id 674
config netuser guest-role apply 675
config netuser guest-role create 676
config netuser guest-role delete 677
config netuser guest-role qos data-rate average-data-rate 678
config netuser guest-role qos data-rate average-realtime-rate 679
config netuser guest-role qos data-rate burst-data-rate 680
config netuser guest-role qos data-rate burst-realtime-rate 681
config netuser lifetime 682
config netuser maxUserLogin 683
config netuser password 684
config netuser wlan-id 685
config network bridging-shared-secret 686
config network web-auth captive-bypass 687
config network web-auth port 688
config network web-auth proxy-redirect 689
config network web-auth secureweb 690
config network webmode 691
config network web-auth 692
config network 802.3-bridging 693
config network allow-old-bridge-aps 694
config network ap-discovery 695
config network ap-easyadmin 696

config network ap-fallback 697
config network ap-priority 698
config network apple-talk 699
config network arptimeout 700
config assisted-roaming 701
config network allow-old-bridge-aps 702
config network ap-discovery 703
config network ap-fallback 704
config network ap-priority 705
config network apple-talk 706
config network bridging-shared-secret 707
config network bridging-shared-secret 708
config network broadcast 709
config network fast-ssid-change 710
config network ip-mac-binding 711
config network link local bridging 712
config network master-base 713
config network mgmt-via-wireless 714
config network multicast global 715
config network multicast igmp query interval 716
config network multicast igmp snooping 717
config network multicast igmp timeout 718
config network multicast l2mcast 719
config network multicast mld 720
config network multicast mode multicast 721
config network multicast mode unicast 722
config network oeap-600 dual-rlan-ports 723
config network oeap-600 local-network 724
config network otap-mode 725
config network profiling 726
config network rf-network-name 727
config network secureweb 728
config network secureweb cipher-option 729
config network ssh 730

config network telnet 731
config network usertimeout 732
config network web-auth captive-bypass 733
config network web-auth cmcc-support 734
config network web-auth port 735
config network web-auth proxy-redirect 736
config network web-auth secureweb 737
config network web-auth https-redirect 738
config network webmode 739
config network web-auth 740
config network zero-config 741
config network master-base 742
config network oeap-600 dual-rlan-ports 743
config network oeap-600 local-network 744
config network otap-mode 745
config network zero-config 746
config nmsp notify-interval measurement 747
config opendns 748
config opendns api-token 749
config opendns forced 750
config opendns profile 751
config pmipv6 domain 752
config pmipv6 add profile 753
config pmipv6 delete 754
config pmipv6 mag apn 755
config pmipv6 mag binding init-retx-time 756
config pmipv6 mag binding lifetime 757
config pmipv6 mag binding max-retx-time 758
config pmipv6 mag binding maximum 759
config pmipv6 mag binding refresh-time 760
config pmipv6 mag bri delay 761
config pmipv6 mag bri retries 762
config pmipv6 mag lma 763
config pmipv6 mag replay-protection 764

config port power 765
config policy action opendns-profile-name 766
config paging 767
config passwd-cleartext 768
config policy 769
config policy match role 771
config port adminmode 772
config port maxspeed 773
config port linktrap 774
config port multicast appliance 775
config prompt 776
config qos average-data-rate 777
config qos average-realtime-rate 778
config qos burst-data-rate 779
config qos burst-realtime-rate 780
config qos description 781
config qos fastlane 782
config qos fastlane disable global 783
config qos max-rf-usage 784
config qos dot1p-tag 785
config qos priority 786
config qos protocol-type 788
config qos queue_length 789
config qos qosmap 790
config qos qosmap up-to-dscp-map 791
config qos qosmap dscp-to-up-exception 792
config qos qosmap delete-dscp-exception 793
config qos qosmap clear-all 794
config qos qosmap trust dscp upstream 795

CHAPTER 7 **Config Commands: r to z** 797

config radius acct 806
config radius acct ipsec authentication 809
config radius acct ipsec disable 810

config radius acct ipsec enable 811
config radius acct ipsec encryption 812
config radius acct ipsec ike 813
config radius acct mac-delimiter 814
config radius acct network 815
config radius acct realm 816
config radius acct retransmit-timeout 817
config radius auth 818
config radius auth callStationIdType 820
config radius auth framed-mtu 822
config radius auth IPsec authentication 823
config radius auth ipsec disable 824
config radius auth ipsec encryption 825
config radius auth ipsec ike 826
config radius auth keywrap 828
config radius auth mac-delimiter 829
config radius auth management 830
config radius auth mgmt-retransmit-timeout 831
config radius auth network 832
config radius auth realm 833
config radius auth retransmit-timeout 834
config radius auth rfc3576 835
config radius auth retransmit-timeout 836
config radius aggressive-failover disabled 837
config radius backward compatibility 838
config radius callStationIdCase 839
config radius callStationIdType 840
config radius dns 842
config radius fallback-test 843
config radius ext-source-ports 845
config radius acct retransmit-timeout 846
config radius auth mgmt-retransmit-timeout 847
config radius auth retransmit-timeout 848
config radius auth retransmit-timeout 849

config redundancy interface address peer-service-port 850
config redundancy mobilitymac 851
config redundancy mode 852
config redundancy peer-route 853
config redundancy timer keep-alive-timer 854
config redundancy timer peer-search-timer 855
config redundancy unit 856
config remote-lan 857
config remote-lan aaa-override 858
config remote-lan acl 859
config remote-lan apgroup 860
config remote-lan create 861
config remote-lan custom-web 862
config remote-lan delete 864
config remote-lan dhcp_server 865
config remote-lan exclusionlist 866
config remote-lan host-mode 867
config remote-lan interface 868
config remote-lan ldap 869
config remote-lan mac-filtering 870
config remote-lan mab 871
config remote-lan max-associated-clients 872
config remote-lan pre-auth 873
config remote-lan radius_server 874
config remote-lan security 875
config remote-lan session-timeout 876
config remote-lan violation-mode 877
config remote-lan webauth-exclude 878
config rf-profile band-select 879
config rf-profile client-trap-threshold 881
config rf-profile create 882
config rf-profile fra client-aware 883
config rf-profile data-rates 884
config rf-profile delete 885

config rf-profile description 886
config rf-profile fra client-aware 887
config rf-profile load-balancing 888
config rf-profile max-clients 889
config rf-profile multicast data-rate 890
config rf-profile out-of-box 891
config rf-profile rx-sop threshold 892
config rf-profile tx-power-control-thresh-v1 893
config rf-profile tx-power-control-thresh-v2 894
config rf-profile tx-power-max 895
config rf-profile tx-power-min 896
config rogue ap timeout 897
config rogue adhoc 898
config rogue ap classify 901
config rogue ap friendly 903
config rogue ap rldp 905
config rogue ap ssid 907
config rogue ap timeout 909
config rogue auto-contain level 910
config rogue ap valid-client 912
config rogue client 914
config rogue containment 916
config rogue detection 917
config rogue detection client-threshold 918
config rogue detection min-rssi 919
config rogue detection monitor-ap 920
config rogue detection report-interval 922
config rogue detection security-level 923
config rogue detection transient-rogue-interval 924
config rogue rule 925
config rogue rule condition ap 929
config remote-lan session-timeout 931
config rfid auto-timeout 932
config rfid status 933

config rfid timeout 934
config rogue ap timeout 935
config route add 936
config route delete 937
config serial baudrate 938
config serial timeout 939
config service timestamps 940
config sessions maxsessions 941
config sessions timeout 942
config slot 943
config switchconfig boot-break 944
config switchconfig fips-prerequisite 945
config switchconfig ucapl 946
config switchconfig wlancc 947
config switchconfig strong-pwd 948
config switchconfig flowcontrol 951
config switchconfig mode 952
config switchconfig secret-obfuscation 953
config sysname 954
config snmp community accessmode 955
config snmp community create 956
config snmp community delete 957
config snmp community ipaddr 958
config snmp community mode 959
config snmp engineID 960
config snmp syscontact 961
config snmp syslocation 962
config snmp trapreceiver create 963
config snmp trapreceiver delete 964
config snmp trapreceiver mode 965
config snmp v3user create 966
config snmp v3user delete 968
config snmp version 969
config tacacs acct 970

config tacacs auth 972
config tacacs auth mgmt-server-timeout 974
config tacacs dns 975
config tacacs fallback-test interval 976
config time manual 977
config time ntp 978
config time timezone 981
config time timezone location 982
config trapflags 802.11-Security 985
config trapflags aaa 986
config trapflags adjchannel-rogueap 987
config trapflags ap 988
config trapflags authentication 989
config trapflags client 990
config trapflags client max-warning-threshold 991
config trapflags configsave 992
config trapflags IPsec 993
config trapflags linkmode 994
config trapflags mesh 995
config trapflags multiusers 996
config trapflags rfid 997
config trapflags rogueap 999
config trapflags rrm-params 1000
config trapflags rrm-profile 1001
config trapflags stpmode 1002
config trapflags strong-pwdcheck 1003
config trapflags wps 1004
config tunnel eogre heart-beat 1005
config tunnel eogre gateway 1006
config tunnel eogre domain 1007
config tunnel eogre domain primary 1008
config tunnel profile 1009
config tunnel profile_rule 1010
config tunnel profile_rule-delete 1011

config tunnel profile eogre-DHCP82 **1012**
config tunnel profile eogre-gateway-radius-proxy **1013**
config tunnel profile eogre-gateway-radius-proxy-accounting **1014**
config tunnel profile eogre-DHCP82 **1015**
config tunnel profile eogre-DHCP82-circuit-id **1016**
config tunnel profile eogre-DHCP82-delimiter **1017**
config tunnel profile eogre-DHCP82-format **1018**
config tunnel profile eogre-DHCP82-remote-id **1019**
config watchlist add **1020**
config watchlist delete **1021**
config watchlist disable **1022**
config watchlist enable **1023**
config wgb vlan **1024**
config wlan **1025**
config wlan 7920-support **1026**
config wlan 802.11e **1027**
config wlan aaa-override **1028**
config wlan acl **1029**
config wlan apgroup **1030**
config wlan apgroup atf 802.11 **1037**
config wlan apgroup atf 802.11 policy **1038**
config wlan apgroup opendns-profile **1039**
config wlan apgroup qinq **1040**
config wlan assisted-roaming **1041**
config wlan atf **1042**
config wlan avc **1043**
config wlan band-select allow **1044**
config wlan broadcast-ssid **1045**
config wlan call-snoop **1046**
config wlan chd **1047**
config wlan ccx aironet-ie **1048**
config wlan channel-scan defer-priority **1049**
config wlan channel-scan defer-time **1050**
config wlan custom-web **1051**

config wlan dhcp_server 1053
config wlan diag-channel 1054
config wlan dtim 1055
config wlan exclusionlist 1056
config wlan fabric 1057
config wlan fabric acl 1058
config wlan fabric avc-policy 1059
config wlan fabric encap vxlan 1060
config wlan fabric switch-ip 1061
config wlan fabric tag 1062
config wlan fabric vnid 1063
config wlan flexconnect ap-auth 1064
config wlan flexconnect central-assoc 1065
config wlan flexconnect learn-ipaddr 1066
config wlan flexconnect local-switching 1067
config wlan flexconnect vlan-central-switching 1069
config wlan flow 1070
config wlan hotspot 1071
config wlan hotspot dot11u 1072
config wlan hotspot dot11u 3gpp-info 1073
config wlan hotspot dot11u auth-type 1074
config wlan hotspot dot11u disable 1075
config wlan hotspot dot11u domain 1076
config wlan hotspot dot11u enable 1077
config wlan hotspot dot11u hessid 1078
config wlan hotspot dot11u ipaddr-type 1079
config wlan hotspot dot11u nai-realm 1080
config wlan hotspot dot11u network-type 1083
config wlan hotspot dot11u roam-oi 1084
config wlan hotspot hs2 1085
config wlan hotspot hs2 domain-id 1088
config wlan hotspot hs2 osu legacy-ssid 1089
config wlan hotspot hs2 osu sp create 1090
config wlan hotspot hs2 osu sp delete 1091

config wlan hotspot hs2 osu sp icon-file add 1092
config wlan hotspot hs2 osu sp icon-file delete 1093
config wlan hotspot hs2 osu sp method add 1094
config wlan hotspot hs2 osu sp method delete 1095
config wlan hotspot hs2 osu sp nai add 1096
config wlan hotspot hs2 osu sp nai delete 1097
config wlan hotspot hs2 osu sp uri add 1098
config wlan hotspot hs2 osu sp uri delete 1099
config wlan hotspot hs2 wan-metrics downlink 1100
config wlan hotspot hs2 wan-metrics link-status 1101
config wlan hotspot hs2 wan-metrics lmd 1102
config wlan hotspot hs2 wan-metrics uplink 1103
config wlan hotspot msap 1104
config wlan interface 1105
config wlan ipv6 acl 1106
config wlan kts-cac 1107
config wlan layer2 acl 1108
config wlan ldap 1109
config wlan learn-ipaddr-cswlan 1110
config wlan load-balance 1111
config wlan lobby-admin-access 1112
config wlan mac-filtering 1113
config wlan max-associated-clients 1114
config wlan max-radio-clients 1115
config wlan mdns 1116
config wlan media-stream 1117
config wlan mfp 1118
config wlan mobility anchor 1119
config wlan mobility foreign-map 1120
config wlan multicast buffer 1121
config wlan multicast interface 1122
config wlan mu-mimo 1123
config wlan nac 1124
config wlan override-rate-limit 1125

config wlan opendns-mode 1127
config wlan opendns-profile 1128
config wlan passive-client 1129
config wlan peer-blocking 1130
config wlan pmipv6 default-realm 1131
config wlan pmipv6 mobility-type 1132
config wlan pmipv6 profile_name 1133
config wlan policy 1134
config wlan profiling 1135
config wlan qos 1136
config wlan radio 1137
config wlan radius_server acct 1138
config wlan radius_server acct interim-update 1139
config wlan radius_server auth 1140
config wlan radius_server overwrite-interface 1141
config wlan radius_server realm 1142
config wlan roamed-voice-client re-anchor 1143
config wlan security 802.1X 1144
config wlan security ckip 1146
config wlan security cond-web-redir 1147
config wlan security eap-params 1148
config wlan security eap-passthru 1150
config wlan security ft 1151
config wlan security ft over-the-ds 1152
config wlan security IPsec disable 1153
config wlan security IPsec enable 1154
config wlan security IPsec authentication 1155
config wlan security IPsec encryption 1156
config wlan security IPsec config 1157
config wlan security IPsec ike authentication 1158
config wlan security IPsec ike dh-group 1159
config wlan security IPsec ike lifetime 1160
config wlan security IPsec ike phase1 1161
config wlan security IPsec ike contivity 1162

config wlan security wpa akm ft 1163
config wlan security ft 1164
config wlan security passthru 1165
config wlan security pmf 1166
config wlan security sgt 1168
config wlan security splash-page-web-redir 1169
config wlan security static-wep-key authentication 1170
config wlan security static-wep-key disable 1171
config wlan security static-wep-key enable 1172
config wlan security static-wep-key encryption 1173
config wlan security tkip 1174
config wlan usertimeout 1175
config wlan security web-auth 1176
config wlan security web-auth captive-bypass 1178
config wlan security web-auth qrscan-des-key 1179
config wlan security web-passthrough acl 1180
config wlan security web-passthrough disable 1181
config wlan security web-passthrough email-input 1182
config wlan security web-passthrough enable 1183
config wlan security web-passthrough qr-scan 1184
config wlan security wpa akm 802.1x 1185
config wlan security wpa akm cckm 1186
config wlan security wpa akm ft 1187
config wlan security wpa akm pmf 1188
config wlan security wpa akm psk 1189
config wlan security wpa disable 1190
config wlan security wpa enable 1191
config wlan security wpa ciphers 1192
config wlan security wpa gtk-random 1193
config wlan security wpa osen disable 1194
config wlan security wpa osen enable 1195
config wlan security wpa wpa1 disable 1196
config wlan security wpa wpa1 enable 1197
config wlan security wpa wpa2 disable 1198

config wlan security wpa wpa2 enable 1199
config wlan security wpa wpa2 cache 1200
config wlan security wpa wpa2 cache sticky 1201
config wlan security wpa wpa2 ciphers 1202
config wlan session-timeout 1203
config wlan sip-cac disassoc-client 1204
config wlan sip-cac send-486busy 1205
config wlan static-ip tunneling 1206
config wlan uapsd compliant client enable 1207
config wlan uapsd compliant-client disable 1208
config wlan url-acl 1209
config wlan user-idle-threshold 1210
config wlan usertimeout 1211
config wlan webauth-exclude 1212
config wlan wgb broadcast-tagging 1213
config wlan wifidirect 1214
config wlan wmm 1215
config wps ap-authentication 1216
config wps auto-immune 1217
config wps cids-sensor 1218
config wps client-exclusion 1220
config wps mfp 1221
config wps shun-list re-sync 1222
config wps signature 1223
config wps signature frequency 1225
config wps signature interval 1226
config wps signature mac-frequency 1227
config wps signature quiet-time 1228
config wps signature reset 1229

PART IV **Debug Commands** 1231

CHAPTER 8 **Debug Commands: 802.11** 1233

debug 11k 1234

debug 11w-pmf 1235
debug 11v all 1236
debug 11v detail 1237
debug 11v error 1238
debug 11w-pmf 1239

CHAPTER 9 **Debug Commands: a to i** 1241

debug aaa 1243
debug aaa events 1244
debug aaa local-auth 1245
debug airewave-director 1247
debug ap 1249
debug ap enable 1251
debug ap packet-dump 1252
debug ap show stats 1253
debug ap show stats video 1255
debug arp 1256
debug avc 1257
debug bcast 1258
debug call-control 1259
debug capwap 1260
debug capwap reap 1261
debug ccxdiag 1262
debug ccxrm 1263
debug ccxs69 1264
debug cckm 1265
debug client 1266
debug cts aaa 1267
debug cts authz 1268
debug cts capwap 1269
debug cts env-data 1270
debug cts ha 1271
debug cts key-store 1272
debug cts provisioning 1273

debug cts sgt 1274
debug cts sxp 1275
debug cac 1276
debug cdp 1277
debug crypto 1278
debug dhcp 1279
debug dhcp service-port 1280
debug disable-all 1281
debug dns 1282
debug dot11 1283
debug dot11 1284
debug dot11 mgmt interface 1285
debug dot11 mgmt msg 1286
debug dot11 mgmt ssid 1287
debug dot11 mgmt state-machine 1288
debug dot11 mgmt station 1289
debug dot1x 1290
debug dtls 1291
debug fastpath 1292
debug flexconnect avc 1297
debug flexconnect aaa 1298
debug flexconnect acl 1299
debug flexconnect cckm 1300
debug group 1301
debug fmchs 1302
debug flexconnect client ap 1303
debug flexconnect client ap syslog 1304
debug flexconnect client group 1305
debug flexconnect client group syslog 1306
debug flexconnect group 1307
debug ft 1308
debug hotspot 1309
debug ipv6 1310

CHAPTER 10 **Debug Commands: j to q** 1311

debug l2age 1312
debug mac 1313
debug mdns all 1314
debug mdns detail 1315
debug mdns error 1316
debug mdns message 1317
debug mdns ha 1318
debug memory 1319
debug mesh security 1320
debug mobility 1321
debug nac 1323
debug nmsp 1324
debug ntp 1325
debug packet error 1326
debug packet logging 1327
debug pem 1330
debug pm 1331
debug poe 1333
debug policy 1334
debug profiling 1335

CHAPTER 11 **Debug Commands: r to z** 1337

debug rbcp 1338
debug rfid 1339
debug snmp 1340
debug transfer 1341
debug voice-diag 1342
debug wcp 1343
debug web-auth 1344
debug wips 1345
debug wps sig 1346
debug wps mfp 1347

PART V IMM Commands 1349

CHAPTER 12 IMM Commands 1351

imm address 1352

imm dhcp 1353

imm mode 1354

imm restart 1355

imm summary 1356

imm username 1357

PART VI License Commands 1359

CHAPTER 13 License Commands 1361

license activate ap-count eval 1362

license activate feature 1363

license add ap-count 1364

license add feature 1365

license clear 1366

license comment 1367

license deactivate ap-count eval 1368

license deactivate feature 1369

license delete ap-count 1370

license delete feature 1371

license install 1372

license modify priority 1373

license revoke 1375

license save 1376

license smart 1377

PART VII Show Commands 1379

CHAPTER 14 Show Commands: 802.11 1381

show 802.11 1382

show 802.11 1384
show 802.11 cleanair 1386
show 802.11 cleanair air-quality summary 1388
show 802.11 cleanair air-quality worst 1389
show 802.11 cleanair device ap 1390
show 802.11 cleanair device type 1391
show 802.11 cu-metrics 1393
show 802.11 extended 1394
show 802.11 media-stream 1395

CHAPTER 15 Show Commands: a to i 1397
show aaa auth 1401
show acl 1402
show acl detailed 1404
show acl url-acl detailed 1405
show acl summary 1406
show acl url-acl summary 1407
show advanced 802.11 channel 1408
show advanced 802.11 coverage 1409
show advanced 802.11 group 1410
show advanced hyperlocation summary 1411
show advanced hyperlocation ble-beacon 1412
show advanced 802.11 l2roam 1413
show advanced 802.11 logging 1414
show advanced 802.11 monitor 1415
show advanced 802.11 optimized roaming 1416
show advanced 802.11 profile 1417
show advanced 802.11 receiver 1418
show advanced 802.11 summary 1419
show advanced 802.11 txpower 1420
show advanced backup-controller 1421
show advanced dot11-padding 1422
show advanced hotspot 1423
show advanced max-1x-sessions 1424

show advanced probe 1425
show advanced rate 1426
show advanced timers 1427
show advanced client-handoff 1428
show advanced eap 1429
show advanced fra 1430
show advanced send-disassoc-on-handoff 1432
show advanced sip-preferred-call-no 1433
show advanced sip-snooping-ports 1434
show arp kernel 1435
show arp switch 1436
show ap auto-rf 1437
show ap aid-audit-mode 1439
show ap ccx rm 1440
show ap cdp 1441
show ap channel 1443
show ap config 1444
show ap config general 1450
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 image status 1461
show ap inventory 1462
show ap join stats detailed 1463
show ap join stats summary 1464
show ap join stats summary all 1465
show ap led-state 1466
show ap led-flash 1467

show ap link-encryption 1468
show ap max-count summary 1469
show ap monitor-mode summary 1470
show ap module summary 1471
show ap packet-dump status 1472
show ap prefer-mode stats 1473
show ap retransmit 1474
show ap stats 1475
show ap summary 1478
show ap tcp-mss-adjust 1479
show ap wlan 1480
show assisted-roaming 1481
show atf config 1482
show atf statistics ap 1483
show auth-list 1484
show avc applications 1485
show avc profile 1486
show avc statistics application 1487
show avc statistics client 1489
show avc statistics guest-lan 1491
show avc statistics remote-lan 1492
show avc statistics top-apps 1493
show avc statistics wlan 1495
show boot 1497
show band-select 1498
show buffers 1499
show cac voice stats 1501
show cac voice summary 1502
show cac video stats 1503
show cac video summary 1505
show call-control ap 1506
show call-control client 1509
show call-home summary 1510
show capwap reap association 1511

show capwap reap status 1512
show cdp 1513
show certificate compatibility 1514
show certificate lsc 1515
show certificate ssc 1516
show certificate summary 1517
show client ap 1518
show client calls 1519
show client ccx client-capability 1520
show client ccx frame-data 1521
show client ccx last-response-status 1522
show client ccx last-test-status 1523
show client ccx log-response 1524
show client ccx manufacturer-info 1525
show client ccx operating-parameters 1526
show client ccx profiles 1527
show client ccx results 1529
show client ccx rm 1530
show client ccx stats-report 1532
show client detail 1533
show client location-calibration summary 1537
show client probing 1538
show client roam-history 1539
show client summary 1540
show client summary guest-lan 1542
show client tsm 1543
show client username 1545
show client voice-diag 1546
show client wlan 1547
show cloud-services cmx summary 1548
show cloud-services cmx statistics 1549
show cts ap 1550
show cts environment-data 1551
show cts pacs 1552

show cts policy 1553
show cts sgacl 1554
show cts summary 1555
show cts sxp 1556
show coredump summary 1557
show country 1558
show country channels 1559
show country supported 1560
show cpu 1562
show custom-web 1563
show database summary 1564
show dhcp 1565
show dhcp proxy 1566
show dhcp timeout 1567
show dtls connections 1568
show exclusionlist 1569
show fabric summary 1570
show flexconnect acl detailed 1572
show flexconnect acl summary 1573
show flexconnect group detail 1574
show flexconnect group summary 1575
show flexconnect office-extend 1576
show flow exporter 1577
show flow monitor summary 1578
show guest-lan 1579
show icons summary 1580
show ike 1581
show interface summary 1582
show interface detailed 1583
show interface group 1585
show invalid-config 1587
show inventory 1588
show IPsec 1589
show ipv6 acl 1591

show ipv6 summary 1592
show guest-lan 1593
show icons file-info 1594
show ipv6 acl 1595
show ipv6 acl cpu 1596
show ipv6 acl detailed 1597
show ipv6 neighbor-binding 1598
show ipv6 ra-guard 1602
show ipv6 route summary 1603
show ipv6 summary 1604
show known ap 1605

CHAPTER 16 Show Commands: j to q 1607
show l2tp 1610
show lag eth-port-hash 1611
show lag ip-port-hash 1612
show lag summary 1613
show ldap 1614
show ldap statistics 1615
show ldap summary 1616
show license all 1617
show license capacity 1619
show license detail 1620
show license expiring 1621
show license evaluation 1622
show license feature 1623
show license file 1624
show license handle 1625
show license image-level 1626
show license in-use 1627
show license permanent 1628
show license status 1629
show license statistics 1630
show license summary 1631

show license udi 1632
show license usage 1633
show load-balancing 1634
show local-auth config 1635
show local-auth statistics 1637
show local-auth certificates 1639
show logging 1640
show logging config-history 1642
show logging last-reset 1643
show logging flags 1644
show loginsession 1645
show macfilter 1646
show mdns ap summary 1647
show mdns domain-name-ip summary 1648
show mdns profile 1650
show mdns service 1652
show media-stream client 1654
show media-stream group detail 1655
show media-stream group summary 1656
show mesh ap 1657
show mesh astools stats 1658
show mesh backhaul 1659
show mesh bgscan 1660
show mesh cac 1661
show mesh client-access 1663
show mesh config 1664
show mesh env 1665
show mesh neigh 1666
show mesh path 1669
show mesh per-stats 1670
show mesh public-safety 1671
show mesh queue-stats 1672
show mesh security-stats 1673
show mesh stats 1674

show mgmtuser 1675
show mobility anchor 1676
show mobility ap-list 1677
show mobility foreign-map 1678
show mobility group member 1679
show mobility oracle 1680
show mobility statistics 1682
show mobility summary 1683
show msglog 1685
show nac statistics 1686
show nac summary 1687
show network 1688
show network summary 1689
show netuser 1691
show netuser guest-roles 1692
show network multicast mgid detail 1693
show network multicast mgid summary 1694
show network summary 1695
show nmsp notify-interval summary 1697
show nmsp status 1698
show nmsp statistics 1699
show nmsp subscription 1701
show nmsp subscription summary 1702
show ntp-keys 1703
show ntp-keys 1704
show opendns summary 1705
show pmk-cache 1706
show pmipv6 domain 1707
show pmipv6 mag bindings 1708
show pmipv6 mag globals 1709
show pmipv6 mag stats 1710
show pmipv6 profile summary 1712
show policy 1713
show port 1715

show profiling policy summary 1717
show qos 1720
show qos qosmap 1721
show queue-info 1722

CHAPTER 17 **Show Commands: r to z** 1725
show radius acct detailed 1728
show radius acct statistics 1729
show radius auth detailed 1730
show radius auth statistics 1731
show radius avp-list 1732
show radius summary 1733
show redundancy interfaces 1734
show redundancy latency 1735
show redundancy mobilitymac 1736
show redundancy peer-route summary 1737
show redundancy peer-system statistics 1738
show redundancy statistics 1739
show redundancy summary 1740
show redundancy timers 1741
show remote-lan 1742
show reset 1744
show rfid client 1745
show rfid config 1746
show rfid detail 1747
show rfid summary 1748
show rf-profile summary 1749
show rf-profile details 1750
show rogue adhoc custom summary 1753
show rogue adhoc detailed 1754
show rogue adhoc friendly summary 1755
show rogue adhoc malicious summary 1756
show rogue adhoc unclassified summary 1757
show rogue adhoc summary 1758

show rogue ap clients 1759
show rogue ap custom summary 1761
show rogue ap detailed 1763
show rogue ap friendly summary 1766
show rogue ap malicious summary 1768
show rogue ap summary 1770
show rogue ap unclassified summary 1773
show rogue auto-contain 1774
show rogue client detailed 1775
show rogue client summary 1776
show rogue ignore-list 1777
show rogue rule detailed 1779
show rogue rule summary 1781
show route kernel 1782
show route summary 1783
show rules 1784
show run-config 1785
show run-config startup-commands 1786
show serial 1787
show sessions 1788
show snmpcommunity 1789
show snmpengineID 1790
show snmptrap 1791
show snmpv3user 1792
show snmpversion 1793
show spanningtree port 1794
show spanningtree switch 1795
show stats port 1796
show stats switch 1798
show switchconfig 1800
show sysinfo 1801
show tacacs acct statistics 1803
show tacacs auth statistics 1804
show tacacs summary 1805

show tech-support 1806
show time 1807
show trapflags 1809
show traplog 1811
show tunnel profile summary 1812
show tunnel profile-detail 1813
show tunnel eogre-summary 1814
show tunnel eogre-statistics 1815
show tunnel eogre-domain-summary 1816
show tunnel eogre gateway 1817
show watchlist 1818
show wlan 1819
show wps ap-authentication summary 1824
show wps cids-sensor 1825
show wps mfp 1826
show wps shun-list 1827
show wps signature detail 1828
show wps signature events 1829
show wps signature summary 1831
show wps summary 1833
show wps wips statistics 1835
show wps wips summary 1836
show wps ap-authentication summary 1837

PART VIII Miscellaneous Commands 1839

CHAPTER 18 Miscellaneous Commands: 1 1841
cping 1842
eping 1843
mping 1844
ping 1845

CHAPTER 19 Miscellaneous Commands: 2 1847
capwap ap controller ip address 1849

config ap dhcp release-override 1850
capwap ap dot1x 1851
capwap ap hostname 1852
capwap ap ip address 1853
capwap ap ip default-gateway 1854
capwap ap log-server 1855
capwap ap primary-base 1856
capwap ap primed-timer 1857
capwap ap secondary-base 1858
capwap ap tertiary-base 1859
lwapp ap controller ip address 1860
reset system at 1861
reset system in 1862
reset system cancel 1863
reset system notify-time 1864
reset peer-system 1865
save config 1866
transfer download certpasswor 1867
transfer download datatype 1868
transfer download datatype icon 1869
transfer download filename 1870
transfer download mode 1871
transfer download password 1872
transfer download path 1873
transfer download port 1874
transfer download serverip 1875
transfer download start 1876
transfer download tftpPktTimeout 1877
transfer download tftpMaxRetries 1878
transfer download username 1879
transfer encrypt 1880
transfer upload datatype 1881
transfer upload filename 1883
transfer upload mode 1884

transfer upload pac 1885
transfer upload password 1886
transfer upload path 1887
transfer upload peer-start 1888
transfer upload port 1889
transfer upload serverip 1890
transfer upload start 1891
transfer upload username 1892

Preface

This preface describes the audience, organization, and conventions of the *Cisco Wireless LAN Controller Command Reference Guide*. It also provides information on how to obtain other documentation.

This preface includes the following sections:

- Audience, on page liii
- Document Conventions, on page liii
- Related Documentation, on page lvi
- Communications, Services, and Additional Information, on page lvi

Audience

This publication is for experienced network administrators who configure and maintain Cisco wireless controllers and Cisco lightweight access points (Cisco APs).

Note Usage of **test** commands may cause system disruption such as an unexpected reboot of the controller. Therefore, we recommend that you use the **test** commands on controllers for debugging purposes with the help of Cisco Technical Assistance Center (TAC) personnel.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Indication
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

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

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

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")

Warning Title	Description
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).)

Warning Title	Description
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").
¡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].)

Related Documentation

These documents provide complete information about the Cisco Unified Wireless Network solution:

- *Cisco Wireless LAN Controller Configuration Guide*
- *Cisco Wireless LAN Controller System Message Guide*
- *Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points*

Communications, Services, and Additional Information

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

Cisco Bug Search Tool

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

Documentation Feedback

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

PART I

Using the Command-Line Interface

- Using the Command-Line Interface, on page 1

Using the Command-Line Interface

This chapter contains the following topics:

- CLI Command Keyboard Shortcuts, on page 2
- Using the Interactive Help Feature, on page 4

CLI Command Keyboard Shortcuts

The table below lists the CLI keyboard shortcuts to help you enter and edit command lines on the controller.

Table 1: CLI Command Keyboard Shortcuts

Action	Description	Keyboard Shortcut
Change	The word at the cursor to lowercase.	Esc I
	The word at the cursor to uppercase.	Esc u
Delete	A character to the left of the cursor.	Ctrl-h, Delete, or Backspace
	All characters from the cursor to the beginning of the line.	Ctrl-u
	All characters from the cursor to the end of the line.	Ctrl-k
	All characters from the cursor to the end of the word.	Esc d
	The word to the left of the cursor.	Ctrl-w or Esc Backspace
Display MORE output	Exit from MORE output.	q, Q, or Ctrl-C
	Next additional screen. The default is one screen. To display more than one screen, enter a number before pressing the Spacebar key.	Spacebar
	Next line. The default is one line. To display more than one line, enter the number before pressing the Enter key.	Enter
Enter or Return key character.		Ctrl-m
Expand the command or abbreviation.		Ctrl-t or Tab
Move the cursor	One character to the left (back).	Ctrl-b or Left Arrow
	One character to the right (forward).	Ctrl-f or Right Arrow
	One word to the left (back), to the beginning of the current or previous word.	Esc b
	One word to the right (forward), to the end of the current or next word.	Esc f
	To the beginning of the line.	Ctrl-a
	To the end of the line.	Ctrl-e
Redraw the screen at the prompt.		Ctrl-l or Ctrl-r

Action	Description	Keyboard Shortcut
Return to the EXEC mode from any configuration mode		Ctrl-z
Return to the previous mode or exit from the CLI from Exec mode.		exit command
Transpose a character at the cursor with a character to the left of the cursor.		Ctrl-t

Using the Interactive Help Feature

The question mark (?) character allows you to get the following type of help about the command at the command line. The table below lists the interactive help feature list.

Table 2: Interactive Help Feature List

Command	Description
help	Provides a brief description of the Help feature in any command mode.
? at the command prompt	Lists all commands available for a particular command mode.
partial command?	Provides a list of commands that begin with the character string.
partial command<Tab>	Completes a partial command name.
command ?	Lists the keywords, arguments, or both associated with a command.
command keyword ?	Lists the arguments that are associated with the keyword.

Using the help Command

Before you begin

To look up keyboard commands, use the help command at the root level.

help

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must back up until entering a '?' shows the available options. Two types of help are available:

1. Full help is available when you are ready to enter a command argument (for example show ?) and describes each possible argument.
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (for example show pr?).

Example:

```
> 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
```

Using the ? command

Before you begin

To display all of the commands in your current level of the command tree, or to display more information about a particular command, use the ? command.

command name **?**

When you enter a command information request, put a space between the **command name** and **?**.

Examples

This command shows you all the commands and levels available from the root level.

```
> ?
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.
```

Using the partial? command

Before you begin

To provide a list of commands that begin with the character string, use the partial command ?.

partial command?

There should be no space between the command and the question mark.

This example shows how to provide a command that begin with the character string “ad”:

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

The command that matches with the string “ad” is as follows:

```
advanced
```

Using the partial command<tab>

Before you begin

To completes a partial command name, use the partial command<tab> command.

partial command<tab>

There should be no space between the command and <tab>.

This example shows how to complete a partial command name that begin with the character string “cert”:

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

Using the command ?

Examples

To list the keywords, arguments, or both associated with the command, use the command ?.

command-name ?

There should be a space between the command and the question mark.

This example shows how to list the arguments and keyword for the command acl:

```
Controller >config acl ?
```

Information similar to the following appears:

```
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
```

command keyword ?

To list the arguments that are associated with the keyword, use the command keyword ?:

command keyword ?

There should be space between the keyword and the question mark.

This example shows how to display the arguments associated with the keyword cpu:

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

Information similar to the following appears:

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

PART II

Clear Commands

- Clear Commands: a to l, on page 9
- Clear Commands: m to z, on page 29

Clear Commands: a to l

- clear advanced, on page 10
- clear acl counters, on page 11
- clear ap config, on page 12
- clear ap eventlog, on page 13
- clear ap join stats, on page 14
- clear arp, on page 15
- clear ap tsm, on page 16
- clear atf, on page 17
- clear avc statistics, on page 18
- clear client tsm, on page 20
- clear config, on page 21
- clear ext-webauth-url, on page 22
- clear location rfid, on page 23
- clear location statistics rfid, on page 24
- clear locp statistics, on page 25
- clear login-banner, on page 26
- clear lwapp private-config, on page 27

clear advanced

To reset EDCA parameters, packet parameters, or optimized roaming statistics to their deault values, use **clear advanced** command.

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

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
optimized-roaming stats	Clear the 802.11a optimized roaming statistics.
packet	Clear the 802.11a packet parameters configuration.
edca-parameter	Clear the 802.11a edca-parameter configuration.

Command Default

None

The following example shows how to reset edca-parameter values to default:

```
(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

To clear the current counters for an Access Control List (ACL), use the **clear acl counters** command.

clear acl counters *acl_name*

Syntax Description

acl_name	ACL name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the current counters for acl1:

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

clear ap config

To clear (reset to the default values) a lightweight access point's configuration settings, use the **clear ap config** command.

clear ap config *ap_name*

Syntax Description

ap_name	Access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Entering this command does not clear the static IP address of the access point.

The following example shows how to clear the access point's configuration settings for the access point named ap1240_322115:

```
(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

To delete the existing event log and create an empty event log file for a specific access point or for all access points joined to the controller, use the **clear ap eventlog** command.

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

Syntax Description

specific	Specifies a specific access point log file.
ap_name	Name of the access point for which the event log file is emptied.
all	Deletes the event log for all access points joined to the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the event log for all access points:

```
(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

To clear the join statistics for all access points or for a specific access point, use the **clear ap join stats** command.

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

Syntax Description

all	Specifies all access points.
ap_mac	Access point MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the join statistics of all the access points:

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

clear arp

To clear the Address Resolution Protocol (ARP) table, use the **clear arp** command.

clear arp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the ARP table:

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

Related Commands

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

To clear the Traffic Stream Metrics (TSM) statistics of clients associated to an access point, use the **clear ap tsm** command.

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

Syntax Description

802.11a	Clears 802.11a TSM statistics of clients associated to an access point.
802.11b	Clears 802.11b TSM statistics of clients associated to an access point.
cisco_ap	Cisco lightweight access point.
all	Clears TSM statistics of clients associated to the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear 802.11a TSM statistics for all clients of an access point:

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

clear atf

To clear Cisco Airtime Fairness configuration or statistics, use the **clear atf** command.

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

Syntax Description

config	Clears Cisco ATF configuration
statistics	Clears Cisco ATF statistics

Command History

Release	Modification
8.1	This command was introduced

The following is a sample output of the **clear atf config** command:

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

clear avc statistics

To clear Application Visibility and Control (AVC) statistics of a client, guest LAN, remote LAN, or a WLAN use the **clear avc statistics** command.

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

Syntax Description

client	Clears AVC statistics of a client.
all	Clears AVC statistics of all clients.
client-mac	MAC address of a client.
guest-lan	Clears AVC statistics of a guest LAN.
all	Clears AVC statistics of all guest LANs.
guest-lan-id	Guest LAN Identifier between 1 and 5.
remote-lan	Clears AVC statistics of a remote LAN.
all	Clears AVC statistics of all remote LANs.
remote-lan-id	Remote LAN Identifier between 1 and 512.
wlan	Clears AVC statistics of a WLAN.
all	Clears AVC statistics of all WLANs.
wlan-id	WLAN Identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the AVC statistics of a client:

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

Related Commands

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

To clear the Traffic Stream Metrics (TSM) statistics for a particular access point or all the access points to which this client is associated, use the **clear client tsm** command.

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

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
client_mac	MAC address of the client.
ap_mac	MAC address of a Cisco lightweight access point.
all	Specifies all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98:

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

Related Commands

clear upload start

clear config

To reset configuration data to factory defaults, use the **clear config** command.

clear config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the configuration data to factory defaults:

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

Related Commands

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

To clear the external web authentication URL, use the **clear ext-webauth-url** command.

clear ext-webauth-url

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the external web authentication URL:

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

Related Commands

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

To clear a specific Radio Frequency Identification (RFID) tag or all of the RFID tags in the entire database, use the **clear location rfid** command.

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

Syntax Description

mac_address	MAC address of a specific RFID tag.
all	Specifies all the RFID tags in the database.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear all the RFID tags in the database:

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

Related Commands

clear location statistics rfid

config location

show location

show location statistics rfid

clear location statistics rfid

To clear Radio Frequency Identification (RFID) statistics, use the **clear location statistics rfid** command.

clear location statistics rfid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear RFID statistics:

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

Related Commands

config location

show location

show location statistics rfid

clear locp statistics

To clear the Location Protocol (LOCP) statistics, use the **clear locp statistics** command.

clear locp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics related to LOCP:

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

Related Commands

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

clear login-banner

To remove the login banner file from the controller, use the **clear login-banner** command.

clear login-banner

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the login banner file:

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

Related Commands

transfer download datatype

clear lwapp private-config

To clear (reset to default values) an access point's current Lightweight Access Point Protocol (LWAPP) private configuration, which contains static IP addressing and controller IP address configurations, use the **clear lwapp private-config** command.

clear lwapp private-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Enter the command on the access point console port.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

The following example shows how to clear an access point's current LWAPP private configuration:

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

Clear Commands: m to z

- clear mdns service-database, on page 30
- clear nmsp statistics, on page 31
- clear radius acct statistics, on page 32
- clear tacacs auth statistics, on page 33
- clear redirect-url, on page 34
- clear stats ap wlan, on page 35
- clear stats local-auth, on page 36
- clear stats mobility, on page 37
- clear stats port, on page 38
- clear stats radius, on page 39
- clear stats smart-lic, on page 40
- clear stats switch, on page 41
- clear stats tacacs, on page 42
- clear transfer, on page 43
- clear traplog, on page 44
- clear urlacl-counters, on page 45
- clear webimage, on page 46
- clear webmessage, on page 47
- clear webtitle, on page 48

clear mdns service-database

To clear the multicast DNS service database, use the **clear mdns service-database** command.

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

Syntax Description

all	Clears the mDNS service database.
service-name	Name of the mDNS service. The controller clears the details of the mDNS service.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database.

The following example shows how to clear the mDNS service database:

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

Related Commands

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

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command.

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the NMSP statistics log file:

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

Related Commands

clear locp statistics

config nmsp notify-interval measurement

show nmsp notify-interval summary

show nmsp status

clear radius acct statistics

To clear the RADIUS accounting statistics on the controller, use the **clear radius acc statistics** command.

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

Syntax Description

index	(Optional) Specifies the index of the RADIUS accounting server.
all	(Optional) Specifies all RADIUS accounting servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the RADIUS accounting statistics:

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

Related Commands

show radius acct statistics

clear tacacs auth statistics

To clear the RADIUS authentication server statistics in the controller, use the **clear tacacs auth statistics** command.

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

Syntax Description

index	(Optional) Specifies the index of the RADIUS authentication server.
all	(Optional) Specifies all RADIUS authentication servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the RADIUS authentication server statistics:

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

Related Commands

show tacacs auth statistics

show tacacs summary

config tacacs auth

clear redirect-url

To clear the custom web authentication redirect URL on the Cisco Wireless LAN Controller, use the **clear redirect-url** command.

clear redirect-url

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication redirect URL:

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

Related Commands

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

To clear the WLAN statistics, use the **clear stats ap wlan** command.

clear stats ap wlan *cisco_ap*

Syntax Description

cisco_ap	Selected configuration elements.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the WLAN configuration elements of the access point cisco_ap:

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

clear stats local-auth

To clear the local Extensible Authentication Protocol (EAP) statistics, use the **clear stats local-auth** command.

clear stats local-auth

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the local EAP statistics:

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

Related Commands

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

To clear mobility manager statistics, use the **clear stats mobility** command.

clear stats mobility

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear mobility manager statistics:

```
(Cisco Controller) >clear stats mobility

   Mobility stats cleared.
```

clear stats port

To clear statistics counters for a specific port, use the **clear stats port** command.

clear stats port *port*

Syntax Description

port	Physical interface port number.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics counters for port 9:

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

Related Commands

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

To clear the statistics for one or more RADIUS servers, use the **clear stats radius** command.

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

Syntax Description

auth	Clears statistics regarding authentication.
acct	Clears statistics regarding accounting.
index	Specifies the index number of the RADIUS server to be cleared.
all	Clears statistics for all RADIUS servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the statistics for all RADIUS authentication servers:

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

Related Commands

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

To clear all the Cisco Smart Software statistics, use the **clear stats smart-lic** command.

clear stats smart-lic

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to clear smart licensing statistics:

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

Initiated Smart Licensing statistics clear
```

clear stats switch

To clear all switch statistics counters on a Cisco wireless LAN controller, use the **clear stats switch** command.

clear stats switch

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear all switch statistics counters:

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

Related Commands

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

To clear the TACACS+ server statistics on the controller, use the **clear stats tacacs** command.

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

Syntax Description

auth	(Optional) Clears the TACACS+ authentication server statistics.
athr	(Optional) Clears the TACACS+ authorization server statistics.
acct	(Optional) Clears the TACACS+ accounting server statistics.
index	(Optional) Specifies index of the TACACS+ server.
all	(Optional) Specifies all TACACS+ servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the TACACS+ accounting server statistics for index 1:

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

Related Commands

show tacacs summary

clear transfer

To clear the transfer information, use the **clear transfer** command.

clear transfer

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the transfer information:

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

Related Commands

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

To clear the trap log, use the **clear traplog** command.

clear traplog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the trap log:

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

Related Commands

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 urlacl-counters

To clear the URL ACL counters for given acl name, use the **clear urlacl-counters** command.

clear urlacl-counters

Syntax Description

acl_name	ACL name.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to clear the URL ACL counters for acl name - test:

```
(Cisco Controller) >clear urlacl-counters test
```

clear webimage

To clear the custom web authentication image, use the **clear webimage** command.

clear webimage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication image:

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

Related Commands

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

To clear the custom web authentication message, use the **clear webmessage** command.

clear webmessage

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication message:

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

Related Commands

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

To clear the custom web authentication title, use the **clear webtitle** command.

clear webtitle

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the custom web authentication title:

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

Related Commands

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

PART III

Config Commands

- Config Commands: 802.11, on page 51
- Config Commands: a to i, on page 163
- Config Commands: j to q, on page 551
- Config Commands: r to z, on page 797

Config Commands: 802.11

- config 802.11-abgn, on page 54
- config 802.11a 11acsupport, on page 55
- config 802.11-a antenna extAntGain, on page 56
- config 802.11-a channel ap, on page 57
- config 802.11-a txpower ap, on page 58
- config 802.11 antenna diversity, on page 59
- config 802.11 antenna extAntGain, on page 60
- config 802.11 antenna mode, on page 61
- config 802.11 antenna selection, on page 62
- config 802.11b 11gSupport, on page 63
- config 802.11b preamble, on page 64
- config 802.11h channelswitch, on page 65
- config 802.11h powerconstraint, on page 66
- config 802.11h setchannel, on page 67
- config 802.11 11nsupport, on page 68
- config 802.11 11nsupport a-mpdu tx priority, on page 69
- config 802.11 11nsupport a-mpdu tx scheduler, on page 71
- config 802.11 11nsupport antenna, on page 72
- config 802.11 11nsupport guard-interval, on page 73
- config 802.11 11nsupport mcs tx, on page 74
- config 802.11 11nsupport rifs, on page 76
- config 802.11 antenna diversity, on page 77
- config 802.11 antenna extAntGain, on page 78
- config 802.11 antenna mode, on page 79
- config 802.11 antenna selection, on page 80
- config 802.11 channel, on page 81
- config 802.11 channel ap, on page 83
- config 802.11 chan_width, on page 84
- config 802.11 rx-sop threshold, on page 86
- config 802.11 txPower, on page 87
- config 802.11 beamforming, on page 89
- config 802.11h channelswitch, on page 90
- config 802.11h powerconstraint, on page 91

- config 802.11h setchannel, on page 92
- config 802.11h smart dfs, on page 93
- config 802.11 11nsupport, on page 94
- config 802.11 11nsupport a-mpdu tx priority, on page 95
- config 802.11 11nsupport a-mpdu tx scheduler, on page 97
- config 802.11 11nsupport antenna, on page 98
- config 802.11 11nsupport guard-interval, on page 99
- config 802.11 11nsupport mcs tx, on page 100
- config 802.11 11nsupport rifs, on page 102
- config 802.11 beacon period, on page 103
- config 802.11 cac defaults, on page 104
- config 802.11 cac video acm, on page 106
- config 802.11 cac video cac-method, on page 108
- config 802.11 cac video load-based, on page 110
- config 802.11 cac video max-bandwidth, on page 112
- config 802.11 cac media-stream, on page 114
- config 802.11 cac multimedia, on page 116
- config 802.11 cac video roam-bandwidth, on page 118
- config 802.11 cac video sip, on page 120
- config 802.11 cac video tspec-inactivity-timeout, on page 122
- config 802.11 cac voice acm, on page 123
- config 802.11 cac voice max-bandwidth, on page 124
- config 802.11 cac voice roam-bandwidth, on page 126
- config 802.11 cac voice tspec-inactivity-timeout, on page 128
- config 802.11 cac voice load-based, on page 130
- config 802.11 cac voice max-calls, on page 132
- config 802.11 cac voice sip bandwidth, on page 134
- config 802.11 cac voice sip codec, on page 136
- config 802.11 cac voice stream-size, on page 138
- config 802.11 cleanair, on page 140
- config 802.11 cleanair device, on page 142
- config 802.11 cleanair alarm, on page 144
- config 802.11 disable, on page 146
- config 802.11 dtpc, on page 147
- config 802.11 enable, on page 148
- config 802.11 exp-bwreq, on page 149
- config 802.11 fragmentation, on page 150
- config 802.11 l2roam rf-params, on page 151
- config 802.11 max-clients, on page 153
- config 802.11 media-stream multicast-direct, on page 154
- config 802.11 media-stream video-redirect, on page 156
- config 802.11 multicast data-rate, on page 157
- config 802.11 rate, on page 158
- config 802.11 rssi-check, on page 159
- config 802.11 rssi-threshold, on page 160
- config 802.11 tsm, on page 161

• config 802.11b preamble, on page 162

config 802.11-abgn

To configure dual-band radio parameters on an access point, use the **config 802.11-abgn** command.

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

Syntax Description

cleanair	Configures CleanAir on the dual-band radio.
enable	Enables CleanAir for both 2.4-GHz and 5-GHz radios.
disable	Disables CleanAir for both 2.4-GHz and 5-GHz radios.
cisco_ap	Name of the access point to which the command applies.
band	Configures the radio band.
band	Radio band that can be 2.4-GHz or 5-GHz.
enable	Enables the dual-band radio on an access point.
disable	Disables the dual-band radio on an access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Only Cisco CleanAir-enabled access point radios can be configured for Cisco CleanAir.

The following example shows how to enable Cisco CleanAir on an access point:

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

config 802.11a 11acsupport

To configure 802.11ac 5-GHz parameters, use the **config 802.11a 11acsupport**

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

Syntax Description

enable	Enables 802.11ac 5-GHz mode.
disable	Disables 802.11ac 5-GHz mode.
mcs tx	Configures 802.11ac 5-GHz Modulation and Coding Scheme (MCS) rates at which data can be transmitted between the access point and the client.
tx	Configures 802.11ac 5-GHz MCS transmit rates.
mcs_index	MCS index value of 8 or 9. MCS data rates with index 8 or 9 are specific to 802.11ac. When you enable an MCS data rate with index 9, the data rate with MCS index 8 is automatically enabled.
ss	Configures the 802.11ac 5-GHz MCS spatial stream (SS).
spatial_stream	Spatial stream within which you can enable or disable an MCS data rate. Signals transmitted by the various antennae are multiplexed by using different spaces within the same spectral channel. These spaces are known as spatial streams. Three spatial streams are available within which you can enable or disable a MCS rate. The range is from 1 to 3.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Disabling the 802.11n/ac mode applies only to access radios. Backhaul radios always have 802.11n/ac mode enabled if they are 802.11n capable.

The following example shows how to configure the MCS index for spatial stream 3:

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

config 802.11-a antenna extAntGain

To configure the external antenna gain for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a antenna extAntGain** commands.

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

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
ant_gain	Value in .5-dBi units (for instance, 2.5 dBi = 5).
cisco_ap	Name of the access point to which the command applies.
global	Specifies the antenna gain value to all channels.
channel_no	Antenna gain value for a specific channel.

Command Default

Channel properties are disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you enter the **config 802.11-a antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11-a disable** command.

After you configure the external antenna gain, use the **config 802.11-a enable** command to reenable the 802.11 Cisco radio.

The following example shows how to configure an 802.11-a49 external antenna gain of 10 dBi for AP1:

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

config 802.11-a channel ap

To configure the channel properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a channel ap** command.

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

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
cisco_ap	Name of the access point to which the command applies.
global	Enables the Dynamic Channel Assignment (DCA) on all 4.9-GHz and 5.8-GHz subband radios.
channel_no	Custom channel for a specific mesh access point. The range is 1 through 26, inclusive, for a 4.9-GHz band and 149 through 165, inclusive, for a 5.8-GHz band.

Command Default

Channel properties are disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the channel properties:

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

config 802.11-a txpower ap

To configure the transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point, use the **config 802.11-a txpower ap** command.

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

Syntax Description

802.11-a49	Specifies the 4.9-GHz public safety channel.
802.11-a58	Specifies the 5.8-GHz public safety channel.
txpower	Configures transmission power properties.
ap	Configures access point channel settings.
cisco_ap	Name of the access point to which the command applies.
global	Applies the transmission power value to all channels.
power_level	Transmission power value to the designated mesh access point. The range is from 1 to 5.

Command Default

The default transmission power properties for the 4.9-GHz and 5.8-GHz public safety channels on an access point is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an 802.11-a49 transmission power level of 4 for AP1:

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

config 802.11 antenna diversity

To configure the diversity option for 802.11 antennas, use the **config 802.11 antenna diversity** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable antenna diversity for AP01 on an 802.11b network:

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

The following example shows how to enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point left port (sideA):

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

config 802.11 antenna extAntGain

To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command.

config 802.11{**a** | **b**} **antenna extAntGain** *antenna_gain cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
antenna_gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you enter the **config 802.11 antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the external antenna gain, use the **config 802.11 enable** command to enable the 802.11 Cisco radio.

The following example shows how to configure an *802.11a* external antenna gain of *0.5 dBm* for *AP1*:

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

config 802.11 antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

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

config 802.11 antenna selection

To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna.
external	Specifies the external antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure access point AP02 on an 802.11b network to use the internal antenna:

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

config 802.11b 11gSupport

To enable or disable the Cisco wireless LAN solution 802.11g network, use the **config 802.11b 11gSupport** command.

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

Syntax Description

enable	Enables the 802.11g network.
disable	Disables the 802.11g network.

Command Default

The default network for Cisco wireless LAN solution 802.11g is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you enter the **config 802.11b 11gSupport** {**enable** | **disable**} command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the support for the 802.11g network, use the **config 802.11 enable** command to enable the 802.11 radio.

Note To disable an 802.11a, 802.11b and/or 802.11g network for an individual wireless LAN, use the **config wlan radio** command.

The following example shows how to enable the 802.11g network:

```
(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

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

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

Syntax Description

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

The default 802.11b preamble value is short.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Note You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

This command can be used any time that the CLI interface is active.

The following example shows how to change the 802.11b preamble to short:

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

config 802.11h channelswitch

To configure an 802.11h channel switch announcement, use the **config 802.11h channelswitch** command.

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

Syntax Description

enable	Enables the 802.11h channel switch announcement.
disable	Disables the 802.11h channel switch announcement.

Command Default

None

Command History

Release	Modification
7.6	• This command was introduced in a release earlier than Release 7.6. • The **loud** and **quiet** parameters were introduced.

The following example shows how to disable an 802.11h switch announcement:

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

config 802.11h powerconstraint

To configure the 802.11h power constraint value, use the **config 802.11h powerconstraint** command.

config 802.11h powerconstraint *value*

Syntax Description

value	802.11h power constraint value.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the 802.11h power constraint to 5:

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

config 802.11h setchannel

To configure a new channel using 802.11h channel announcement, use the **config 802.11h setchannel** command.

config 802.11h setchannel *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a new channel using the 802.11h channel:

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

config 802.11 11nsupport

To enable 802.11n support on the network, use the **config 802.11 11nsupport** command.

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

Syntax Description

a	Specifies the 802.11a network settings.
b	Specifies the 802.11b/g network settings.
enable	Enables the 802.11n support.
disable	Disables the 802.11n support.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the 802.11n support on an 802.11a network:

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

config 802.11 11nsupport a-mpdu tx priority

To specify the aggregation method used for 802.11n packets, use the **config 802.11 11nsupport a-mpdu tx priority** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
0-7	Specifies the aggregated MAC protocol data unit priority level between 0 through 7.
all	Configures all of the priority levels at once.
enable	Specifies the traffic associated with the priority level uses A-MPDU transmission.
disable	Specifies the traffic associated with the priority level uses A-MSDU transmission.

Command Default

Priority 0 is enabled.

Usage Guidelines

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU is performed in the software whereas A-MSDU is performed in the hardware.

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 1—Background
- 2—Spare
- 0—Best effort
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.

Note Configure the priority levels to match the aggregation method used by the clients.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure all the priority levels at once so that the traffic associated with the priority level uses A-MSDU transmission:

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

config 802.11 11nsupport a-mpdu tx scheduler

To configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler, use the **config 802.11 11nsupport a-mpdu tx scheduler** command.

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

Syntax Description

enable	Enables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
disable	Disables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
timeout rt	Configures the A-MPDU transmit aggregation scheduler realtime traffic timeout.
timeout-value	Timeout value in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.

Command Default

None

Usage Guidelines

Ensure that the 802.11 network is disabled before you enter this command.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the A-MPDU transmit aggregation scheduler realtime traffic timeout of 100 milliseconds:

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

config 802.11 11nsupport antenna

To configure an access point to use a specific antenna, use the **config 802.11 11nsupport antenna** command.

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

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
cisco_ap	Access point.
A/B/C/D	Specifies an antenna port.
enable	Enables the configuration.
disable	Disables the configuration.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure transmission to a single antenna for legacy orthogonal frequency-division multiplexing:

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

config 802.11 11nsupport guard-interval

To configure the guard interval, use the **config 802.11 11nsupport guard-interval** command.

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

Syntax Description

any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a long guard interval:

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

config 802.11 11nsupport mcs tx

To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, use the **config 802.11 11nsupport mcs tx** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
11nsupport	Specifies support for 802.11n devices.
mcs tx	Specifies the modulation and coding scheme data rates as follows: • 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	Enables this configuration.
disable	Disables this configuration.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify MCS rates:

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

config 802.11 11nsupport rifs

To configure the Reduced Interframe Space (RIFS) between data frames and its acknowledgment, use the **config 802.11 11nsupport rifs** command.

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

Syntax Description

enable	Enables RIFS for the 802.11 network.
disable	Disables RIFS for the 802.11 network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable RIFS:

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

config 802.11 antenna diversity

To configure the diversity option for 802.11 antennas, use the **config 802.11 antenna diversity** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the diversity.
sideA	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point left port.
sideB	Specifies the diversity between the internal antennas and an external antenna connected to the Cisco lightweight access point right port.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable antenna diversity for AP01 on an 802.11b network:

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

The following example shows how to enable diversity for AP01 on an 802.11a network, using an external antenna connected to the Cisco lightweight access point left port (sideA):

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

config 802.11 antenna extAntGain

To configure external antenna gain for an 802.11 network, use the **config 802.11 antenna extAntGain** command.

config 802.11{**a** | **b**} **antenna extAntGain** *antenna_gain cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
antenna_gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you enter the **config 802.11 antenna extAntGain** command, disable the 802.11 Cisco radio with the **config 802.11 disable** command.

After you configure the external antenna gain, use the **config 802.11 enable** command to enable the 802.11 Cisco radio.

The following example shows how to configure an *802.11a* external antenna gain of *0.5 dBm* for *AP1*:

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

config 802.11 antenna mode

To configure the Cisco lightweight access point to use one internal antenna for an 802.11 sectorized 180-degree coverage pattern or both internal antennas for an 802.11 360-degree omnidirectional pattern, use the **config 802.11 antenna mode** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
omni	Specifies to use both internal antennas.
sectorA	Specifies to use only the side A internal antenna.
sectorB	Specifies to use only the side B internal antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on an 802.11b network:

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

config 802.11 antenna selection

To select the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network, use the **config 802.11 antenna selection** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
internal	Specifies the internal antenna.
external	Specifies the external antenna.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure access point AP02 on an 802.11b network to use the internal antenna:

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

config 802.11 channel

To configure an 802.11 network or a single access point for automatic or manual channel selection, use the **config 802.11 channel** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies the 802.11a operating channel that is automatically set by RRM and overrides the existing configuration setting.
auto	(Optional) Specifies that the channel is automatically set by Radio Resource Management (RRM) for the 802.11a radio.
once	(Optional) Specifies that the channel is automatically set once by RRM.
off	(Optional) Specifies that the automatic channel selection by RRM is disabled.
restarts	(Optional) Restarts the aggressive DCA cycle.
ap_name	Access point name.
channel	Manual channel number to be used by the access point. The supported channels depend on the specific access point used and the regulatory region.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When configuring 802.11 channels for a single lightweight access point, enter the **config 802.11 disable** command to disable the 802.11 network. Enter the **config 802.11 channel** command to set automatic channel selection by Radio Resource Management (RRM) or manually set the channel for the 802.11 radio, and enter the **config 802.11 enable** command to enable the 802.11 network.

Note See the Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points document for the channels supported by your access point. The power levels and available channels are defined by the country code setting and are regulated on a country-by-country basis.

The following example shows how to have RRM automatically configure the 802.11a channels for automatic channel configuration based on the availability and interference:

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

The following example shows how to configure the 802.11b channels one time based on the availability and interference:

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

The following example shows how to turn 802.11a automatic channel configuration off:

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

The following example shows how to configure the 802.11b channels in access point AP01 for automatic channel configuration:

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

The following example shows how to configure the 802.11a channel 36 in access point AP01 as the default channel:

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

config 802.11 channel ap

To set the operating radio channel for an access point, use the **config 802.11 channel ap** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Name of the Cisco access point.
global	Enables auto-RF on the designated access point.
channel_no	Default channel from 1 to 26, inclusive.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable auto-RF for access point AP01 on an 802.11b network:

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

config 802.11 chan_width

To configure the channel width for a particular access point, use the **config 802.11 chan_width** command.

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

Syntax Description

a	Configures the 802.11a radio on slot 1 and 802.11ac radio on slot 2.
b	Specifies the 802.11b/g radio.
cisco_ap	Access point.
20	Allows the radio to communicate using only 20-MHz channels. Choose this option for legacy 802.11a radios, 20-MHz 802.11n radios, or 40-MHz 802.11n radios that you want to operate using only 20-MHz channels.
40	Allows 40-MHz 802.11n radios to communicate using two adjacent 20-MHz channels bonded together.
80	Allows 80-MHz 802.11ac radios to communicate using two adjacent 40-MHz channels bonded together.
160	Allows 160-MHz 802.11ac radios to communicate.
best	In this mode, the device selects the optimum bandwidth channel.

Command Default

The default channel width is 20.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced in this release with the inclusion of 160 MHz and best channel bandwidth modes.

Usage Guidelines

This parameter can be configured only if the primary channel is statically assigned.

Caution We recommend that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe co-channel interference can occur.

Statically configuring an access point's radio for 20-MHz or 40-MHz mode overrides the globally configured DCA channel width setting (configured by using the **config advanced 802.11 channel dca chan-width**

command). If you change the static configuration back to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

The following example shows how to configure the channel width for access point AP01 on an 802.11 network using 40-MHz channels:

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

config 802.11 rx-sop threshold

To configure the threshold values for Receiver Start of Packet Detection Threshold (RxSOP) for each 802.11 band, use the **config 802.11 rx-sop threshold** command.

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

Syntax Description

802.11a	Configures an RxSOP threshold value for the 802.11a network.
802.11b	Configures an RxSOP threshold value for the 802.11b network.
high	Configures the high RxSOP threshold value for 802.11a/b networks.
medium	Configures the medium RxSOP threshold value for 802.11a/b networks.
low	Configures the low RxSOP threshold value for 802.11a/b networks.
auto	Configures an auto RxSOP threshold value for 802.11a/b networks. When you choose auto, the access point determines the best RxSOP threshold value.
ap *ap_name*	Configures the RxSOP threshold value on an access point of an 802.11 network.
default	Configures the RxSOP threshold value on all access points of an 802.11 network.

Command Default

The default RxSOP threshold option is auto.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

RxSOP determines the Wi-Fi signal level in dBm at which an access point's radio demodulates and decodes a packet. Higher the level, less sensitive the radio is and smaller the receiver cell size. The table below shows the RxSOP threshold values for high, medium and low levels for each 802.11 band.

Table 3: RxSOP Thresholds

802.11 Band	High Threshold	Medium Threshold	Low Threshold
5 GHz	–76 dBm	–78 dBm	–80 dBm
2.4 GHz	–79 dBm	–82 dBm	–85 dBm

The following example shows how to configure a high RxSOP threshold value for all access points in the 802.11a band:

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

config 802.11 txPower

To configure the transmit power level for all access points or a single access point in an 802.11 network, use the **config 802.11 txPower** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures the 802.11 transmit power level for all lightweight access points.
auto	(Optional) Specifies the power level is automatically set by Radio Resource Management (RRM) for the 802.11 Cisco radio.
once	(Optional) Specifies the power level is automatically set once by RRM.
power_level	(Optional) Manual Transmit power level number for the access point.
ap	Configures the 802.11 transmit power level for a specified lightweight access point.
ap_name	Access point name.

Command Default

The command default (**global**, **auto**) is for automatic configuration by RRM.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The supported power levels depends on the specific access point used and the regulatory region. For example, the 1240 series access point supports eight levels and the 1200 series access point supports six levels. See the Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points document for the maximum transmit power limits for your access point. The power levels and available channels are defined by the country code setting and are regulated on a country-by-country basis.

The following example shows how to automatically set the 802.11a radio transmit power level in all lightweight access points:

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

The following example shows how to manually set the 802.11b radio transmit power to level 5 for all lightweight access points:

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

The following example shows how to automatically set the 802.11b radio transmit power for access point AP1:

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

The following example shows how to manually set the 802.11a radio transmit power to power level 2 for access point AP1:

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

Related Commands

show ap config 802.11a

config 802.11b txPower

config 802.11 beamforming

To enable or disable Beamforming (ClientLink) on the network or on individual radios, enter the **config 802.11 beamforming** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies all lightweight access points.
ap *ap_name*	Specifies the Cisco access point name.
enable	Enables beamforming.
disable	Disables beamforming.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable Beamforming on the network, it is automatically enabled for all the radios applicable to that network type.

Follow these guidelines for using Beamforming:

- Beamforming is supported only for legacy orthogonal frequency-division multiplexing (OFDM) data rates (6, 9, 12, 18, 24, 36, 48, and 54 mbps).

Note Beamforming is not supported for complementary-code keying (CCK) data rates (1, 2, 5.5, and 11 Mbps).

- Beamforming is supported only on access points that support 802.11n (AP1250 and AP1140).
- Two or more antennas must be enabled for transmission.
- All three antennas must be enabled for reception.
- OFDM rates must be enabled.

  If the antenna configuration restricts operation to a single transmit antenna, or if OFDM rates are disabled, Beamforming is not used.

The following example shows how to enable Beamforming on the 802.11a network:

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

config 802.11h channelswitch

To configure an 802.11h channel switch announcement, use the **config 802.11h channelswitch** command.

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

Syntax Description

enable	Enables the 802.11h channel switch announcement.
disable	Disables the 802.11h channel switch announcement.

Command Default

None

Command History

Release	Modification
7.6	• This command was introduced in a release earlier than Release 7.6. • The **loud** and **quiet** parameters were introduced.

The following example shows how to disable an 802.11h switch announcement:

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

config 802.11h powerconstraint

To configure the 802.11h power constraint value, use the **config 802.11h powerconstraint** command.

config 802.11h powerconstraint *value*

Syntax Description

value	802.11h power constraint value.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the 802.11h power constraint to 5:

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

config 802.11h setchannel

To configure a new channel using 802.11h channel announcement, use the **config 802.11h setchannel** command.

config 802.11h setchannel *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a new channel using the 802.11h channel:

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

config 802.11h smart dfs

To enable or disable 802.11h smart-dfs feature, use the **config 802.11h smart-dfs** command.

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

Syntax Description

enable	Enables non occupancy time doubling for Radar interfere channel.
disable	Disables non occupancy time doubling and use legacy time (30 minutes) for Radar interference channel. Use disable to match legacy DFS behavior.

Command Default

Enabled

Command History

Release	Modification
8.2.141.0	This command was introduced.

The following example shows how to enable 802.11h smart-dfs:

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

config 802.11 11nsupport

To enable 802.11n support on the network, use the **config 802.11 11nsupport** command.

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

Syntax Description

a	Specifies the 802.11a network settings.
b	Specifies the 802.11b/g network settings.
enable	Enables the 802.11n support.
disable	Disables the 802.11n support.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the 802.11n support on an 802.11a network:

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

config 802.11 11nsupport a-mpdu tx priority

To specify the aggregation method used for 802.11n packets, use the **config 802.11 11nsupport a-mpdu tx priority** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
0-7	Specifies the aggregated MAC protocol data unit priority level between 0 through 7.
all	Configures all of the priority levels at once.
enable	Specifies the traffic associated with the priority level uses A-MPDU transmission.
disable	Specifies the traffic associated with the priority level uses A-MSDU transmission.

Command Default

Priority 0 is enabled.

Usage Guidelines

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. Two aggregation methods are available: Aggregated MAC Protocol Data Unit (A-MPDU) and Aggregated MAC Service Data Unit (A-MSDU). A-MPDU is performed in the software whereas A-MSDU is performed in the hardware.

Aggregated MAC Protocol Data Unit priority levels assigned per traffic type are as follows:

- 1—Background
- 2—Spare
- 0—Best effort
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 10-ms latency and jitter
- 7—Network control
- all—Configure all of the priority levels at once.

Note Configure the priority levels to match the aggregation method used by the clients.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure all the priority levels at once so that the traffic associated with the priority level uses A-MSDU transmission:

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

config 802.11 11nsupport a-mpdu tx scheduler

To configure the 802.11n-5 GHz A-MPDU transmit aggregation scheduler, use the **config 802.11 11nsupport a-mpdu tx scheduler** command.

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

Syntax Description

enable	Enables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
disable	Disables the 802.11n-5 GHz A-MPDU transmit aggregation scheduler.
timeout rt	Configures the A-MPDU transmit aggregation scheduler realtime traffic timeout.
timeout-value	Timeout value in milliseconds. The valid range is between 1 millisecond to 1000 milliseconds.

Command Default

None

Usage Guidelines

Ensure that the 802.11 network is disabled before you enter this command.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the A-MPDU transmit aggregation scheduler realtime traffic timeout of 100 milliseconds:

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

config 802.11 11nsupport antenna

To configure an access point to use a specific antenna, use the **config 802.11 11nsupport antenna** command.

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

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
cisco_ap	Access point.
A/B/C/D	Specifies an antenna port.
enable	Enables the configuration.
disable	Disables the configuration.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure transmission to a single antenna for legacy orthogonal frequency-division multiplexing:

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

config 802.11 11nsupport guard-interval

To configure the guard interval, use the **config 802.11 11nsupport guard-interval** command.

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

Syntax Description

any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a long guard interval:

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

config 802.11 11nsupport mcs tx

To specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client, use the **config 802.11 11nsupport mcs tx** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
11nsupport	Specifies support for 802.11n devices.
mcs tx	Specifies the modulation and coding scheme data rates as follows: • 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	Enables this configuration.
disable	Disables this configuration.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify MCS rates:

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

config 802.11 11nsupport rifs

To configure the Reduced Interframe Space (RIFS) between data frames and its acknowledgment, use the **config 802.11 11nsupport rifs** command.

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

Syntax Description

enable	Enables RIFS for the 802.11 network.
disable	Disables RIFS for the 802.11 network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable RIFS:

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

config 802.11 beacon period

To change the beacon period globally for an 802.11a, 802.11b, or other supported 802.11 network, use the **config 802.11 beacon period** command.

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

Note Disable the 802.11 network before using this command. See the "Usage Guidelines" section.

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
time_units	Beacon interval in time units (TU). One TU is 1024 microseconds.

Command Default

None

Usage Guidelines

In Cisco wireless LAN solution 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the 802.11a service is available and allows the clients to synchronize with the lightweight access point.

Before you change the beacon period, make sure that you have disabled the 802.11 network by using the **config 802.11 disable** command. After changing the beacon period, enable the 802.11 network by using the **config 802.11 enable** command.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to configure an 802.11a network for a beacon period of 120 time units:

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

Related Commands

show 802.11a

config 802.11b beaconperiod

config 802.11a disable

config 802.11a enable

config 802.11 cac defaults

To configure the default Call Admission Control (CAC) parameters for the 802.11a and 802.11b/g network, use the **config 802.11 cac defaults** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to configure the default CAC parameters for the 802.11a network:

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

Related Commands

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

To enable or disable video Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac video acm** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables video CAC settings.
disable	Disables video CAC settings.

Command Default

The default video CAC settings for the 802.11a or 802.11b/g network is disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable**, or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the video CAC for the 802.11a network:

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

The following example shows how to disable the video CAC for the 802.11b network:

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

Related Commands

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

To configure the Call Admission Control (CAC) method for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video cac-method** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
static	Enables the static CAC method for video applications on the 802.11a or 802.11b/g network. Static or bandwidth-based CAC enables the client to specify how much bandwidth or shared medium time is required to accept a new video request and in turn enables the access point to determine whether it is capable of accommodating the request.
load-based	Enables the load-based CAC method for video applications on the 802.11a or 802.11b/g network. Load-based or dynamic CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment. The access point admits a new call only if the channel has enough unused bandwidth to support that call. Load-based CAC is not supported if SIP-CAC is enabled.

Command Default

Static.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Video CAC consists of two parts: Unicast Video-CAC and MC2UC CAC. If you need only Unicast Video-CAC, you must configure only static mode. If you need only MC2UC CAC, you must configure Static or Load-based CAC. Load-based CAC is not supported if SIP-CAC is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable the static CAC method for video applications on the 802.11a network:

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

Related Commands

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

To enable or disable load-based Call Admission Control (CAC) for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video load-based** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables load-based CAC for video applications on the 802.11a or 802.11b/g network. Load-based or dynamic CAC incorporates a measurement scheme that takes into account the bandwidth consumed by all traffic types from itself, from co-channel access points, and by collocated channel interference. Load-based CAC also covers the additional bandwidth consumption results from PHY and channel impairment. The access point admits a new call only if the channel has enough unused bandwidth to support that call.
disable	Disables load-based CAC method for video applications on the 802.11a or 802.11b/g network.

Command Default

Disabled.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Video CAC consists of two parts: Unicast Video-CAC and MC2UC CAC. If you need only Unicast Video-CAC, you must configure only static mode. If you need only MC2UC CAC, you must configure Static or Load-based CAC. Load-based CAC is not supported if SIP-CAC is enabled.

Note Load-based CAC is not supported if SIP-CAC is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable load-based CAC method for video applications on the 802.11a network:

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

Related Commands

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

To set the percentage of the maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video max-bandwidth** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The default maximum bandwidth allocated to clients for video applications on the 802.11a or 802.11b/g network is 0%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

Note If this parameter is set to zero (0), the controller assumes that you do not want to allocate any bandwidth and allows all bandwidth requests.

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable**, or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the percentage of the maximum allocated bandwidth for video applications on the selected radio band:

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

Related Commands

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

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 802.11a and 802.11b networks, use the **config 802.11 cac media-stream** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
multicast-direct	Configures CAC parameters for multicast-direct media streams.
max-retry-percent	Configures the percentage of maximum retries that are allowed for multicast-direct media streams.
retry-percentage	Percentage of maximum retries that are allowed for multicast-direct media streams.
min-client-rate	Configures the minimum transmission data rate to the client for multicast-direct media streams.
dot11-rate	Minimum transmission data rate to the client for multicast-direct media streams. Rate in kbps at which the client can operate. If the transmission data rate is below this rate, either the video will not start or the client may be classified as a bad client. The bad client video can be demoted for better effort QoS or subject to denial. The available data rates are 6000, 9000, 12000, 18000, 24000, 36000, 48000, 54000, and 11n rates.

Command Default

The default value for the maximum retry percent is 80. If it exceeds 80, either the video will not start or the client might be classified as a bad client. The bad client video will be demoted for better effort QoS or is subject to denial.

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the maximum retry percent for multicast-direct media streams as 90 on a 802.11a network:

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

Related Commands

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

To configure the CAC media voice and video quality parameters for 802.11a and 802.11b networks, use the **config 802.11 cac multimedia** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
max-bandwidth	Configures the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 802.11a or 802.11b/g network.
bandwidth	Percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a or 802.11b/g network. Once the client reaches the specified value, the access point rejects new calls on this radio band. The range is from 5 to 85%.

Command Default

The default maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 802.11a or 802.11b/g network is 85%.

Usage Guidelines

Call Admission Control (CAC) commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 802.11a network:

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

Related Commands

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

To configure the percentage of the maximum allocated bandwidth reserved for roaming video clients on the 802.11a or 802.11b/g network, use the **config 802.11 cac video roam-bandwidth** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The maximum allocated bandwidth reserved for roaming video clients on the 802.11a or 802.11b/g network is 0%.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming video clients.

Note If this parameter is set to zero (0), the controller assumes that you do not want to do any bandwidth allocation and, therefore, allows all bandwidth requests.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

The following example shows how to specify the percentage of the maximum allocated bandwidth reserved for roaming video clients on the selected radio band:

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

Related Commands

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

To enable or disable video Call Admission Control (CAC) for nontraffic specifications (TSPEC) SIP clients using video applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac video sip** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables video CAC for non-TSPEC SIP clients using video applications on the 802.11a or 802.11b/g network. When you enable video CAC for non-TSPEC SIP clients, you can use applications like Facetime and CIUS video calls.
disable	Disables video CAC for non-TSPEC SIP clients using video applications on the 802.11a or 802.11b/g network.

Command Default

None

Usage Guidelines

CAC commands for video applications on the 802.11a or 802.11b/g network require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Gold.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** command.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.
- Enable call snooping on the WLAN on which the SIP client is present by entering the **config wlan call-snoop enable** *wlan_id* command.

The following example shows how to enable video CAC for non-TSPEC SIP clients using video applications on the 802.11a network:

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

Related Commands

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

To process or ignore the Call Admission Control (CAC) Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac video tspec-inactivity-timeout** command.

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

Syntax Description

a	Specifies the 802.11a network.
ab	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default CAC WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11** {**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11** {**a** | **b**} **cac voice acm enable** or **config 802.11** {**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

This example shows how to process the response to TSPEC inactivity timeout messages received from an access point:

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

This example shows how to ignore the response to TSPEC inactivity timeout messages received from an access point:

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

Related Commands

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

To enable or disable bandwidth-based voice Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice acm** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the bandwidth-based CAC.
disable	Disables the bandwidth-based CAC.

Command Default

The default bandwidth-based voice CAC for the 802.11a or 802.11b/g network id disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

This example shows how to enable the bandwidth-based CAC:

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

This example shows how to disable the bandwidth-based CAC:

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

Related Commands

config 802.11 cac video acm

config 802.11 cac voice max-bandwidth

To set the percentage of the maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice max-bandwidth** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 5 to 85%.

Command Default

The default maximum bandwidth allocated to clients for voice applications on the 802.11a or 802.11b/g network is 0%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. Once the client reaches the value specified, the access point rejects new calls on this network.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the percentage of the maximum allocated bandwidth for voice applications on the selected radio band:

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

Related Commands

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

To configure the percentage of the Call Admission Control (CAC) maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network, use the **config 802.11 cac voice roam-bandwidth** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bandwidth	Bandwidth percentage value from 0 to 85%.

Command Default

The default CAC maximum allocated bandwidth reserved for roaming voice clients on the 802.11a or 802.11b/g network is 85%.

Usage Guidelines

The maximum radio frequency (RF) bandwidth cannot exceed 85% for voice and video. The controller reserves the specified bandwidth from the maximum allocated bandwidth for roaming voice clients.

Note If this parameter is set to zero (0), the controller assumes you do not want to allocate any bandwidth and therefore allows all bandwidth requests.

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the percentage of the maximum allocated bandwidth reserved for roaming voice clients on the selected radio band:

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

Related Commands

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

To process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point, use the **config 802.11 cac voice tspec-inactivity-timeout** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages.

Command Default

The default WMM TSPEC inactivity timeout received from an access point is disabled (ignore).

Usage Guidelines

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the voice TSPEC inactivity timeout messages received from an access point:

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

Related Commands

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

To enable or disable load-based Call Admission Control (CAC) for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice load-based** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables load-based CAC.
disable	Disables load-based CAC.

Command Default

The default load-based CAC for the 802.11a or 802.11b/g network is disabled.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id command*.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the voice load-based CAC parameters:

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

The following example shows how to disable the voice load-based CAC parameters:

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

Related Commands

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

Note Do not use the **config 802.11 cac voice max-calls** command if the SIP call snooping feature is disabled and if the SIP based Call Admission Control (CAC) requirements are not met.

To configure the maximum number of voice call supported by the radio, use the **config 802.11 cac voice max-calls** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
number	Number of calls to be allowed per radio.

Command Default

The default maximum number of voice call supported by the radio is 0, which means that there is no maximum limit check for the number of calls.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id command*.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable network** command.
- Save the new configuration by entering the **save config command.**
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the maximum number of voice calls supported by radio:

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

Related Commands

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

Note SIP bandwidth and sample intervals are used to compute per call bandwidth for the SIP-based Call Admission Control (CAC).

To configure the bandwidth that is required per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip bandwidth** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
bw_kbps	Bandwidth in kbps.
sample-interval	Specifies the packetization interval for SIP codec.
number_msecs	Packetization sample interval in msecs. The sample interval for SIP codec is 20 seconds.

Command Default

None

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the bandwidth and voice packetization interval for a SIP codec:

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

Related Commands

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

To configure the Call Admission Control (CAC) codec name and sample interval as parameters and to calculate the required bandwidth per call for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice sip codec** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
g711	Specifies CAC parameters for the SIP G711 codec.
g729	Specifies CAC parameters for the SIP G729 codec.
sample-interval	Specifies the packetization interval for SIP codec.
number_msecs	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.

Command Default

The default CAC codec parameter is g711.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the codec name and sample interval as parameters for SIP G711 codec:

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

This example shows how to configure the codec name and sample interval as parameters for SIP G729 codec:

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

Related Commands

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

To configure the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 802.11a or 802.11b/g network, use the **config 802.11 cac voice stream-size** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
stream-size	Configures the maximum data rate for the stream.
stream_size	Range of stream size is between 84000 and 92100.
number	Number (1 to 5) of voice streams.
mean_datarate	Configures the mean data rate.
max-streams	Configures the mean data rate of a voice stream.
mean_datarate	Mean data rate (84 to 91.2 kbps) of a voice stream.

Command Default

The default number of streams is 2 and the mean data rate of a stream is 84 kbps.

Usage Guidelines

Call Admission Control (CAC) commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol and the quality of service (QoS) level be set to Platinum.

Before you can configure CAC parameters on a network, you must complete the following prerequisites:

- Disable all WLANs with WMM enabled by entering the **config wlan disable** *wlan_id* command.
- Disable the radio network you want to configure by entering the **config 802.11**{**a** | **b**} **disable** network command.
- Save the new configuration by entering the **save config** command.
- Enable voice or video CAC for the network you want to configure by entering the **config 802.11**{**a** | **b**} **cac voice acm enable** or **config 802.11**{**a** | **b**} **cac video acm enable** commands.

  For complete instructions, see the "Configuring Voice and Video Parameters" section in the "Configuring Controller Settings" chapter of the *Cisco Wireless LAN Controller Configuration Guide* for your release.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the number of aggregated voice traffic specifications stream with the stream size 5 and the mean data rate of 85000 kbps:

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

Related Commands

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

To enable or disable CleanAir for the 802.11 a or 802.11 b/g network, use the **config 802.11 cleanair** command.

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*} }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
alarm	Configure 5-GHz cleanair alarms.
air-quality	Configures the 5-GHz air quality alarm.
enable	Enables the CleanAir settings.
disable	Disables the CleanAir settings.
threshold	Configure the 5-GHz air quality alarm threshold.
alarm_threshold	Air quality alarm threshold (1 is bad air quality, and 100 is good air quality).
device	Configures the 5-GHz cleanair interference devices alarm.

device_type	Device types. The device types are as follows: • 802.11-nonstd—Devices using nonstandard Wi-Fi channels. • 802.11-inv—Devices using spectrally inverted Wi-Fi signals. • superag—802.11 SuperAG devices. • all —All interference device types. • cont-tx—Continuous Transmitter. • dect-like—Digital Enhanced Cordless Communication (DECT) like phone. • tdd-tx—TDD Transmitter. • jammer—Jammer. • canopy—Canopy devices. • video—Video cameras. • wimax-mobile—WiMax Mobile. • wimax-fixed—WiMax Fixed.
reporting	Configures the 5-GHz CleanAir interference devices alarm reporting.
unclassified	Configures the 5-GHz air quality alarm on exceeding unclassified category severity.
network	5-GHz Cisco APs.
cisco_ap	Name of the access point to which the command applies.

Command Default

The default CleanAir settings for the 802.11 a or 802.11 b/g network is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the CleanAir settings on access point ap_24:

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

config 802.11 cleanair device

To configure CleanAir interference device types, use the **config 802.11 cleanair device** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the CleanAir reporting for the interference device type.
disable	Disables the CleanAir reporting for the interference device type.
reporting	Configures CleanAir interference device reporting.
enable	Enables the 5-GHz Cleanair interference devices reporting.
disable	Disables the 5-GHz Cleanair interference devices reporting.
device_type	Interference device type. The device type are as follows: • 802.11-nonstd—Devices using nonstandard WiFi channels. • 802.11-inv—Devices using spectrally inverted WiFi signals. • superag—802.11 SuperAG devices. • all —All interference device types. • cont-tx—Continuous Transmitter. • dect-like—Digital Enhanced Cordless Communication (DECT) like phone. • tdd-tx—TDD Transmitter. • jammer—Jammer. • canopy—Canopy devices. • video—Video cameras. • wimax-mobile—WiMax Mobile. • wimax-fixed—WiMax Fixed.

Command Default

The default setting CleanAir reporting for the interference device type is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the CleanAir reporting for the device type jammer:

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

The following example shows how to disable the CleanAir reporting for the device type video:

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

The following example shows how to enable the CleanAir interference device reporting:

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

config 802.11 cleanair alarm

To configure the triggering of the air quality alarms, use the **config 802.11 cleanair alarm** command.

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* } }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
air-quality	Configures the 5-GHz air quality alarm.
disable	Disables the 5-GHz air quality alarm.
enable	Enables the 5-GHz air quality alarm.
threshold	Configures the 5-GHz air quality alarm threshold.
alarm_threshold	Air quality alarm threshold (1 is bad air quality, and 100 is good air quality).
device	Configures the 5-GHz cleanair interference devices alarm.
all	Configures all the device types at once.
reporting	Configures the 5-GHz CleanAir interference devices alarm reporting.
unclassified	Configures the 5-GHz air quality alarm on exceeding unclassified category severity.

device_type	Device types. The device types are as follows: • 802.11-nonstd—Devices using nonstandard Wi-Fi channels. • 802.11-inv—Devices using spectrally inverted Wi-Fi signals. • superag—802.11 SuperAG devices. • all —All interference device types. • cont-tx—Continuous Transmitter. • dect-like—Digital Enhanced Cordless Communication (DECT) like phone. • tdd-tx—TDD Transmitter. • jammer—Jammer. • canopy—Canopy devices. • video—Video cameras. • wimax-mobile—WiMax Mobile. • wimax-fixed—WiMax Fixed.

Command Default

The default setting for 5-GHz air quality alarm is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the CleanAir alarm to monitor the air quality:

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

The following example shows how to enable the CleanAir alarm for the device type video:

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

The following example shows how to enable alarm reporting for the CleanAir interference devices:

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

config 802.11 disable

To disable radio transmission for an entire 802.11 network or for an individual Cisco radio, use the **config 802.11 disable** command.

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

Syntax Description

a	Configures the 802.11a on slot 1 and 802.11ac radio on slot 2. radio.
b	Specifies the 802.11b/g network.
network	Disables transmission for the entire 802.11a network.
cisco_ap	Individual Cisco lightweight access point radio.

Command Default

The transmission is enabled for the entire network by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

- You must use this command to disable the network before using many config 802.11 commands.
- This command can be used any time that the CLI interface is active.

The following example shows how to disable the entire 802.11a network:

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

The following example shows how to disable access point AP01 802.11b transmissions:

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

config 802.11 dtpc

To enable or disable the Dynamic Transmit Power Control (DTPC) setting for an 802.11 network, use the **config 802.11 dtpc** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the support for this command.
disable	Disables the support for this command.

Command Default

The default DTPC setting for an 802.11 network is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable DTPC for an 802.11a network:

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

config 802.11 enable

To enable radio transmission for an entire 802.11 network or for an individual Cisco radio, use the **config 802.11 enable** command.

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

Syntax Description

a	Configures the 802.11a radioon slot 1 and 802.11ac on slot 2.
b	Specifies the 802.11b/g network.
network	Disables transmission for the entire 802.11a network.
cisco_ap	Individual Cisco lightweight access point radio.

Command Default

The transmission is enabled for the entire network by default.

Usage Guidelines

Use this command with the **config 802.11 disable** command when configuring 802.11 settings.

This command can be used any time that the CLI interface is active.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable radio transmission for the entire 802.11a network:

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

The following example shows how to enable radio transmission for AP1 on an 802.11b network:

```
(Cisco Controller) > config 802.11b enable AP1
```

Related Commands

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

To enable or disable the Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature for an 802.11 radio, use the **config 802.11 exp-bwreq** command.

config 802.11 {**a** | **b**} **exp-bwreq** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the expedited bandwidth request feature.
disable	Disables the expedited bandwidth request feature.

Command Default

The expedited bandwidth request feature is disabled by default.

Usage Guidelines

When this command is enabled, the controller configures all joining access points for this feature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the CCX expedited bandwidth settings:

```
(Cisco Controller) > config 802.11a exp-bwreq enable
Cannot change Exp Bw Req mode while 802.11a network is operational.
```

The following example shows how to disable the CCX expedited bandwidth settings:

```
(Cisco Controller) > config 802.11a exp-bwreq disable
```

Related Commands

show 802.11a

show ap stats 802.11a

config 802.11 fragmentation

To configure the fragmentation threshold on an 802.11 network, use the **config 802.11 fragmentation** command.

config 802.11{**a** | **b**} **fragmentation** *threshold*

Note This command can only be used when the network is disabled using the **config 802.11 disable** command.

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
threshold	Number between 256 and 2346 bytes (inclusive).

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to configure the fragmentation threshold on an 802.11a network with the threshold number of 6500 bytes:

```
(Cisco Controller) > config 802.11a fragmentation 6500
```

Related Commands

config 802.11b fragmentation

show 802.11b

show ap auto-rtf

config 802.11 l2roam rf-params

To configure 802.11a or 802.11b/g Layer 2 client roaming parameters, use the **config 802.11 l2roam rf-params** command.

config 802.11 { **a** | **b** } **l2roam rf-params** { **default** | **custom** *min_rssi roam_hyst scan_thresh trans_time* }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
default	Restores Layer 2 client roaming RF parameters to defa
custom	Configures custom Layer 2 client roaming RF paramet
min_rssi	Minimum received signal strength indicator (RSSI) tha associate to the access point. If the client's average rece threshold, reliable communication is usually impossible and roamed to another access point with a stronger signa is reached. The valid range is –80 to –90 dBm, and the
roam_hyst	How much greater the signal strength of a neighboring the client to roam to it. This parameter is intended to re between access points if the client is physically located two access points. The valid range is 2 to 4 dB, and the
scan_thresh	Minimum RSSI that is allowed before the client should When the RSSI drops below the specified value, the clie access point within the specified transition time. This para method to minimize the time that the client spends in a example, the client can scan slowly when the RSSI is al rapidly when the RSSI is below the threshold. The vali the default value is –72 dBm.
trans_time	Maximum time allowed for the client to detect a suitable to and to complete the roam, whenever the RSSI from th is below the scan threshold. The valid range is 1 to 10 s 5 seconds. **Note** For high-speed client roaming applications we recommend that you set the transition t

Command Default

The default minimum RSSI is -85 dBm. The default signal strength of a neighboring access point is 2 dB. The default scan threshold value is -72 dBm. The default time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam is 5 seconds.

Usage Guidelines

For high-speed client roaming applications in outdoor mesh environments, we recommend that you set the *trans_time* to 1 second.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure custom Layer 2 client roaming parameters on an 802.11a network:

```
(Cisco Controller) > config 802.11 l2roam rf-params custom –80 2 –70 7
```

Related Commands

show advanced 802.11 l2roam

show l2tp

config 802.11 max-clients

To configure the maximum number of clients per access point, use the **config 802.11 max-clients** command.

config 802.11 {**a** | **b**} **max-clients** *max-clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
max-clients	Configures the maximum number of client connections per access point.
max-clients	Maximum number of client connections per access point. The range is from 1 to 200.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the maximum number of clients at 22:

```
(Cisco Controller) > config 802.11 max-clients 22
```

Related Commands

show ap config 802.11a

config 802.11b rate

config 802.11 media-stream multicast-direct

To configure the media stream multicast-direct parameters for the 802.11 networks, use the **config 802.11 media-stream multicast-direct** command.

config 802.11 {**a** | **b**} **media-stream multicast-direct** {**admission-besteffort** {**enable** | **disable**} | {**client-maximum** | **radio-maximum**} {*value* | **no-limit** } | **enable** | **disable**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
admission-besteffort	Admits media stream to best-effort queue.
enable	Enables multicast-direct on a 2.4-GHz or a 5-GHz band.
disable	Disables multicast-direct on a 2.4-GHz or a 5-GHz band.
client-maximum	Specifies the maximum number of streams allowed on a client.
radio-maximum	Specifies the maximum number of streams allowed on a 2.4-GHz or a 5-GHz band.
value	Number of streams allowed on a client or on a 2.4-GHz or a 5-GHz band, between 1 to 20.
no-limit	Specifies the unlimited number of streams allowed on a client or on a 2.4-GHz or a 5-GHz band.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you configure the media stream multicast-direct parameters on a 802.11 network, ensure that the network is nonoperational.

This example shows how to enable a media stream multicast-direct settings on an 802.11a network:

```
> config 802.11a media-stream multicast-direct enable
```

This example shows how to admit the media stream to the best-effort queue:

```
> config 802.11a media-stream multicast-direct admission-besteffort enable
```

This example shows how to set the maximum number of streams allowed on a client:

```
> config 802.11a media-stream multicast-direct client-maximum 10
```

Related Commands

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

To configure the media stream video-redirect for the 802.11 networks, use the **config 802.11 media-stream video-redirect** command.

config 802.11 {**a** | **b**} **media-stream video-redirect** {**enable** | **disable**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
enable	Enables traffic redirection.
disable	Disables traffic redirection.

Command Default

None.

Usage Guidelines

Before you configure the media stream video-redirect on a 802.11 network, ensure that the network is nonoperational.

This example shows how to enable media stream traffic redirection on an 802.11a network:

```
> config 802.11a media-stream video-redirect enable
```

Related Commands

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

To configure the minimum multicast data rate, use the **config 802.11 multicast data-rate** command.

config 802.11 {**a** | **b**} **multicast data-rate** *data_rate* [**ap** *ap_name* | **default**]

Syntax Description

data_rate	Minimum multicast data rates. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that APs will dynamically adjust the number of the buffer allocated for multicast.
ap_name	Specific AP radio in this data rate.
default	Configures all APs radio in this data rate.

Command Default

The default is 0 where the configuration is disabled and the multicast rate is the lowest mandatory data rate and unicast client data rate.

Usage Guidelines

When you configure the data rate without the AP name or **default** keyword, you globally reset all the APs to the new value and update the controller global default with this new data rate value. If you configure the data rate with **default** keyword, you only update the controller global default value and do not reset the value of the APs that are already joined to the controller. The APs that join the controller after the new data rate value is set receives the new data rate value.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure minimum multicast data rate settings:

```
(Cisco Controller) > config 802.11 multicast data-rate 12
```

config 802.11 rate

To set mandatory and supported operational data rates for an 802.11 network, use the **config 802.11 rate** command.

config 802.11{**a** | **b**} **rate** {**disabled** | **mandatory** | **supported**} *rate*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
disabled	Disables a specific data rate.
mandatory	Specifies that a client supports the data rate in order to use the network.
supported	Specifies to allow any associated client that supports the data rate to use the network.
rate	Rate value of 6, 9, 12, 18, 24, 36, 48, or 54 Mbps.

Command Default

None

Usage Guidelines

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to **mandatory**, the client must support it in order to use the network. If a data rate is set as **supported** by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked **supported** in order to associate.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the 802.11b transmission at a mandatory rate at 12 Mbps:

```
(Cisco Controller) > config 802.11b rate mandatory 12
```

Related Commands

show ap config 802.11a

config 802.11b rate

config 802.11 rssi-check

To configure the 802.11 RSSI Low Check feature, use the **config 802.11 rssi-check** command.

config 802.11 {**a** | **b**} **rssi-check** {**enable** | **disable**}

Syntax Description

rssi-check	Configures the RSSI Low Check feature.
enable	Enables the RSSI Low Check feature.
disable	Disables the RSSI Low Check feature.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

config 802.11 rssi-threshold

To configure the 802.11 RSSI Low Check threshold, use the **config 802.11 rssi-threshold** command.

config 802.11{**a** | **b**} **rssi-threshold** *value-in-dBm*

Syntax Description

rssi-threshold	Configures the RSSI Low Check threshold value.
value-in-dBm	RSSI threshold value in dBm. The default value is –80 dBm.

Command Default

The default value of the RSSI Low Check threshold is –80 dBm.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The following example shows how to configure the RSSI threshold value to –70 dBm for an 802.11a network:

```
(Cisco Controller) > config 802.11a rssi-threshold -70
```

config 802.11 tsm

To enable or disable the video Traffic Stream Metric (TSM) option for the 802.11a or 802.11b/g network, use the **config 802.11 tsm** command.

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

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the video TSM settings.
disable	Disables the video TSM settings.

Command Default

By default, the TSM for the 802.11a or 802.11b/g network is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the video TSM option for the 802.11b/g network:

```
(Cisco Controller) > config 802.11b tsm enable
```

The following example shows how to disable the video TSM option for the 802.11b/g network:

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

Related Commands

show ap stats

show client tsm

config 802.11b preamble

To change the 802.11b preamble as defined in subclause 18.2.2.2 to **long** (slower, but more reliable) or **short** (faster, but less reliable), use the **config 802.11b preamble** command.

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

Syntax Description

long	Specifies the long 802.11b preamble.
short	Specifies the short 802.11b preamble.

Command Default

The default 802.11b preamble value is short.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Note You must reboot the Cisco Wireless LAN Controller (reset system) with save to implement this command.

This parameter must be set to **long** to optimize this Cisco wireless LAN controller for some clients, including SpectraLink NetLink telephones.

This command can be used any time that the CLI interface is active.

The following example shows how to change the 802.11b preamble to short:

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

Config Commands: a to i

- config aaa auth, on page 171
- config aaa auth mgmt, on page 172
- config acl apply, on page 173
- config acl counter, on page 174
- config acl create, on page 175
- config acl cpu, on page 176
- config acl delete, on page 177
- config acl layer2, on page 178
- config acl rule, on page 180
- config acl url-acl, on page 182
- config acl url-acl apply, on page 183
- config acl url-acl external-server-ip, on page 184
- config acl url-acl list-type, on page 185
- config acl url-domain, on page 186
- config advanced 802.11 7920VSIEConfig, on page 187
- config advanced 802.11 channel add, on page 188
- config advanced 802.11 channel cleanair-event, on page 189
- config advanced 802.11 channel dca anchor-time, on page 190
- config advanced 802.11 channel dca chan-width-11n, on page 191
- config advanced 802.11 channel dca interval, on page 192
- config advanced 802.11 channel dca min-metric, on page 193
- config advanced 802.11 channel dca sensitivity, on page 194
- config advanced 802.11 channel foreign, on page 196
- config advanced 802.11 channel load, on page 197
- config advanced 802.11 channel noise, on page 198
- config advanced 802.11 channel outdoor-ap-dca, on page 199
- config advanced 802.11 channel pda-prop, on page 200
- config advanced 802.11 channel update, on page 201
- config advanced 802.11 coverage, on page 202
- config advanced 802.11 coverage exception global, on page 203
- config advanced 802.11 coverage fail-rate, on page 204
- config advanced 802.11 coverage level global, on page 205
- config advanced 802.11 coverage packet-count, on page 206

- config advanced 802.11 coverage rssi-threshold, on page 207
- config advanced 802.11 edca-parameters, on page 209
- config advanced 802.11 factory, on page 211
- config advanced 802.11 group-member, on page 212
- config advanced 802.11 group-mode, on page 213
- config advanced 802.11 logging channel, on page 214
- config advanced 802.11 logging coverage, on page 215
- config advanced 802.11 logging foreign, on page 216
- config advanced 802.11 logging load, on page 217
- config advanced 802.11 logging noise, on page 218
- config advanced 802.11 logging performance, on page 219
- config advanced 802.11 logging txpower, on page 220
- config advanced 802.11 monitor channel-list, on page 221
- config advanced 802.11 monitor load, on page 222
- config advanced 802.11 monitor measurement, on page 223
- config advanced 802.11 monitor mode, on page 224
- config advanced 802.11 monitor ndp-type, on page 225
- config advanced 802.11 monitor timeout-factor, on page 226
- config advanced 802.11 optimized roaming, on page 227
- config advanced 802.11 packet, on page 228
- config advanced 802.11 profile clients, on page 230
- config advanced 802.11 profile customize, on page 231
- config advanced 802.11 profile foreign, on page 232
- config advanced 802.11 profile noise, on page 233
- config advanced 802.11 profile throughput, on page 234
- config advanced 802.11 profile utilization, on page 235
- config advanced 802.11 receiver, on page 236
- config advanced 802.11 reporting measurement, on page 237
- config advanced 802.11 tpc-version, on page 238
- config advanced 802.11 tpcv1-thresh, on page 239
- config advanced 802.11 tpcv2-intense, on page 240
- config advanced 802.11 tpcv2-per-chan, on page 241
- config advanced 802.11 tpcv2-thresh, on page 242
- config advanced 802.11 txpower-update, on page 243
- config advanced eap, on page 244
- config advanced fra service-priority, on page 246
- config advanced fra client-aware client-select, on page 247
- config advanced fra client-aware client-reset, on page 248
- config advanced hyperlocation, on page 249
- config advanced hyperlocation apgroup, on page 250
- config advanced hyperlocation ble-beacon, on page 251
- config advanced hyperlocation ble-beacon beacon-id, on page 252
- config advanced hotspot, on page 253
- config advanced timers auth-timeout, on page 254
- config advanced timers eap-timeout, on page 255
- config advanced timers eap-identity-request-delay, on page 256

- config advanced timers, on page 257
- config advanced fastpath fastcache, on page 260
- config advanced fastpath pkt-capture, on page 261
- config advanced sip-preferred-call-no, on page 262
- config advanced sip-snooping-ports, on page 263
- config advanced backup-controller primary, on page 264
- config advanced backup-controller secondary, on page 265
- config advanced client-handoff, on page 266
- config advanced dot11-padding, on page 267
- config advanced assoc-limit, on page 268
- config advanced max-1x-sessions, on page 269
- config advanced rate, on page 270
- config advanced probe filter, on page 271
- config advanced probe limit, on page 272
- config advanced timers, on page 273
- config ap 802.1Xuser, on page 276
- config ap 802.1Xuser delete, on page 277
- config ap 802.1Xuser disable, on page 278
- config advanced dot11-padding, on page 279
- config ap, on page 280
- config ap aid-audit, on page 281
- config ap antenna band-mode, on page 282
- config ap atf 802.11, on page 283
- config ap atf 802.11 client-access airtime-allocation, on page 284
- config ap atf 802.11 policy, on page 285
- config ap autoconvert, on page 286
- config ap bhrate, on page 287
- config ap bridgegroupname, on page 288
- config ap bridging, on page 289
- config ap cdp, on page 290
- config ap cert-expiry-ignore, on page 292
- config ap core-dump, on page 293
- config ap crash-file clear-all, on page 294
- config ap crash-file delete, on page 295
- config ap crash-file get-crash-file, on page 296
- config ap crash-file get-radio-core-dump, on page 297
- config ap dhcp release-override, on page 298
- config ap dtls-cipher-suite, on page 299
- config ap dtls-version, on page 300
- config ap ethernet duplex, on page 301
- config ap ethernet tag, on page 302
- config ap autoconvert, on page 303
- config ap flexconnect central-dhcp, on page 304
- config ap flexconnect local-split, on page 305
- config ap flexconnect module-vlan, on page 306
- config ap flexconnect policy, on page 307

- config ap flexconnect radius auth set, on page 308
- config ap flexconnect vlan, on page 309
- config ap flexconnect vlan add, on page 310
- config ap flexconnect vlan native, on page 311
- config ap flexconnect vlan wlan, on page 312
- config ap flexconnect web-auth, on page 313
- config ap flexconnect web-policy acl, on page 314
- config ap flexconnect wlan, on page 315
- config ap group-name, on page 316
- config ap hotspot, on page 317
- config ap image predownload, on page 324
- config ap image swap, on page 325
- config ap ipsla, on page 326
- config ap led-state, on page 327
- config ap link-encryption, on page 328
- config ap link-latency, on page 329
- config ap location, on page 330
- config ap logging syslog level, on page 331
- config ap logging syslog facility, on page 332
- config ap max-count, on page 334
- config ap mgmtuser add, on page 335
- config ap mgmtuser delete, on page 336
- config ap mode, on page 337
- config ap module3g, on page 339
- config ap monitor-mode, on page 340
- config ap name, on page 341
- config ap packet-dump, on page 342
- config ap port, on page 345
- config ap power injector, on page 346
- config ap power pre-standard, on page 347
- config ap preferred-mode, on page 348
- config ap primary-base, on page 349
- config ap priority, on page 350
- config ap reporting-period, on page 351
- config ap reset, on page 352
- config ap retransmit interval, on page 353
- config ap retransmit count, on page 354
- config ap role, on page 355
- config ap rst-button, on page 356
- config ap secondary-base, on page 357
- config ap sniff, on page 358
- config ap ssh, on page 359
- config ap static-ip, on page 360
- config ap stats-timer, on page 362
- config ap syslog host global, on page 363
- config ap syslog host specific, on page 364

- config ap tcp-mss-adjust, on page 365
- config ap telnet, on page 366
- config ap tertiary-base, on page 367
- config ap tftp-downgrade, on page 368
- config ap username, on page 369
- config ap venue, on page 370
- config ap wlan, on page 374
- config atf 802.11, on page 375
- config atf policy, on page 376
- config auth-list add, on page 377
- config auth-list ap-policy, on page 378
- config auth-list delete, on page 379
- config avc profile create, on page 380
- config avc profile delete, on page 381
- config avc profile rule, on page 382
- config band-select cycle-count, on page 384
- config band-select cycle-threshold, on page 385
- config band-select expire, on page 386
- config band-select client-rssi, on page 387
- config boot, on page 388
- config call-home contact email address, on page 389
- config call-home events, on page 390
- config call-home http-proxy ipaddr, on page 391
- config call-home http-proxy ipaddr 0.0.0.0, on page 392
- config call-home profile, on page 393
- config call-home profile delete, on page 394
- config call-home profile status, on page 395
- config call-home reporting, on page 396
- config call-home tac-profile, on page 397
- config cdp, on page 398
- config certificate, on page 399
- config certificate lsc, on page 400
- config certificate ssc, on page 402
- config certificate use-device-certificate webadmin, on page 403
- config client ccx clear-reports, on page 404
- config client ccx clear-results, on page 405
- config client ccx default-gw-ping, on page 406
- config client ccx dhcp-test, on page 407
- config client ccx dns-ping, on page 408
- config client ccx dns-resolve, on page 409
- config client ccx get-client-capability, on page 410
- config client ccx get-manufacturer-info, on page 411
- config client ccx get-operating-parameters, on page 412
- config client ccx get-profiles, on page 413
- config client ccx log-request, on page 414
- config client ccx send-message, on page 416

- config client ccx stats-request, on page 420
- config client ccx test-abort, on page 421
- config client ccx test-association, on page 422
- config client ccx test-dot1x, on page 423
- config client ccx test-profile, on page 424
- config client deauthenticate, on page 425
- config client location-calibration, on page 426
- config client profiling delete, on page 427
- config cloud-services cmx, on page 428
- config cloud-services server url, on page 429
- config cloud-services server id-token, on page 430
- config coredump, on page 431
- config coredump ftp, on page 432
- config coredump username, on page 433
- config country, on page 434
- config cts, on page 435
- config cts ap, on page 436
- config cts inline-tag, on page 437
- config cts ap override, on page 438
- config cts device-id, on page 439
- config cts refresh, on page 440
- config cts sxp ap connection delete, on page 441
- config cts sxp ap connection peer, on page 442
- config cts sxp ap default password, on page 443
- config cts sxp ap listener, on page 444
- config cts sxp ap reconciliation period, on page 445
- config cts sxp ap retry period, on page 446
- config cts sxp ap speaker, on page 447
- config cts sxp, on page 448
- config cts sxp connection, on page 449
- config cts sxp default password, on page 450
- config cts sxp retry period, on page 451
- config cts sxp version, on page 452
- config cts sxp, on page 453
- config custom-web ext-webauth-mode, on page 454
- config custom-web ext-webauth-url, on page 455
- config custom-web ext-webserver, on page 456
- config custom-web logout-popup, on page 457
- config custom-web qrscan-bypass-opt , on page 458
- config custom-web radiusauth , on page 459
- config custom-web redirectUrl, on page 460
- config custom-web sleep-client, on page 461
- config custom-web webauth-type, on page 462
- config custom-web weblogo, on page 463
- config custom-web webmessage, on page 464
- config custom-web webtitle, on page 465

- config database size, on page 466
- config dhcp, on page 467
- config dhcp opt-82 format, on page 469
- config dhcp opt-82 remote-id, on page 470
- config dhcp proxy, on page 471
- config dhcp timeout, on page 472
- config dx, on page 473
- config exclusionlist, on page 474
- config fabric, on page 475
- config fabric vnid create name, on page 476
- config fabric control-plane enterprise-fabric , on page 477
- config fabric control-plane guest-fabric , on page 478
- config flexconnect [ipv6] acl, on page 479
- config flexconnect [ipv6] acl rule, on page 480
- config flexconnect [ipv6] acl url-domain, on page 482
- config flexconnect arp-caching, on page 483
- config flexconnect avc profile, on page 484
- config flexconnect fallback-radio-shut, on page 485
- config flexconnect group, on page 486
- config flexconnect group vlan, on page 491
- config flexconnect group *group-name* dhcp overridden-interface, on page 492
- config flexconnect group web-auth, on page 493
- config flexconnect group web-policy, on page 494
- config flexconnect join min-latency, on page 495
- config flexconnect office-extend, on page 496
- config flow, on page 497
- config guest-lan, on page 498
- config guest-lan custom-web ext-webauth-url, on page 499
- config guest-lan custom-web global disable, on page 500
- config guest-lan custom-web login_page, on page 501
- config guest-lan custom-web webauth-type, on page 502
- config guest-lan ingress-interface, on page 503
- config guest-lan interface, on page 504
- config guest-lan mobility anchor, on page 505
- config guest-lan nac, on page 506
- config guest-lan security, on page 507
- config interface 3g-vlan, on page 508
- config interface acl, on page 509
- config interface address, on page 510
- config interface address redundancy-management, on page 512
- config interface ap-manager, on page 513
- config interface create, on page 514
- config interface delete, on page 515
- config interface dhcp management, on page 516
- config interface dhcp, on page 518
- config interface dhcp dynamic-interface, on page 519

- config interface dhcp management option-6-opendns , on page 520
- config interface address, on page 521
- config interface group failure-detect, on page 523
- config interface group mdns-profile, on page 524
- config interface guest-lan, on page 525
- config interface hostname, on page 526
- config interface nasid, on page 527
- config interface nat-address, on page 528
- config interface port, on page 529
- config interface quarantine vlan, on page 530
- config interface url-acl, on page 531
- config interface vlan, on page 532
- config interface mdns-profile, on page 533
- config icons delete, on page 535
- config icons file-info, on page 536
- config ipv6 disable, on page 537
- config ipv6 enable, on page 538
- config ipv6 acl, on page 539
- config ipv6 capwap, on page 541
- config ipv6 interface, on page 542
- config ipv6 multicast, on page 544
- config ipv6 neighbor-binding, on page 545
- config ipv6 ns-mcast-fwd, on page 547
- config ipv6 ra-guard, on page 548
- config ipv6 route, on page 549

config aaa auth

To configure the AAA authentication search order for management users, use the **config aaa auth** command.

config aaa auth mgmt [*aaa_server_type1* | *aaa_server_type2*]

Syntax Description

mgmt	Configures the AAA authentication search order for controller management users by specifying up to three AAA authentication server types. The order that the server types are entered specifies the AAA authentication search order.
aaa_server_type	(Optional) AAA authentication server type (**local**, **radius**, or **tacacs**). The **local** setting specifies the local database, the **radius** setting specifies the RADIUS server, and the **tacacs** setting specifies the TACACS+ server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can enter two AAA server types as long as one of the server types is **local**. You cannot enter **radius** and **tacacs** together.

The following example shows how to configure the AAA authentication search order for controller management users by the authentication server type local:

```
(Cisco Controller) > config aaa auth radius local
```

Related Commands

show aaa auth

config aaa auth mgmt

To configure the order of authentication when multiple databases are configured, use the **config aaa auth mgmt** command.

config aaa auth mgmt [**radius** | **tacacs**]

Syntax Description

radius	(Optional) Configures the order of authentication for RADIUS servers.
tacacs	(Optional) Configures the order of authentication for TACACS servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the order of authentication for the RADIUS server:

```
(Cisco Controller) > config aaa auth mgmt radius
```

The following example shows how to configure the order of authentication for the TACACS server:

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

Related Commands

show aaa auth order

config acl apply

To apply an access control list (ACL) to the data path, use the **config acl apply** command.

config acl apply *rule_name*

Syntax Description		
	rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Example

The following example shows how to apply an ACL to the data path:

```
(Cisco Controller) > config acl apply acl01
```

config acl counter

To see if packets are hitting any of the access control lists (ACLs) configured on your controller, use the **config acl counter** command.

config acl counter {**start** | **stop**}

Syntax Description

start	Enables ACL counters on your controller.
stop	Disables ACL counters on your controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

ACL counters are available only on the following controllers: 4400 series, Cisco WiSM, and Catalyst 3750G Integrated Wireless LAN Controller Switch.

The following example shows how to enable ACL counters on your controller:

```
(Cisco Controller) > config acl counter start
```

Related Commands

clear acl counters

show acl detailed

config acl create

To create a new access control list (ACL), use the **config acl create** command.

config acl create *rule_name*

Syntax Description		
	rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to create a new ACL:

```
(Cisco Controller) > config acl create acl01
```

Related Commands **show acl**

config acl cpu

To create a new access control list (ACL) rule that restricts the traffic reaching the CPU, use the **config acl cpu** command.

config acl cpu *rule_name* {**wired** | **wireless** | **both**}

Syntax Description

rule_name	Specifies the ACL name.
wired	Specifies an ACL on wired traffic.
wireless	Specifies an ACL on wireless traffic.
both	Specifies an ACL on both wired and wireless traffic.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command allows you to control the type of packets reaching the CPU.

The following example shows how to create an ACL named acl101 on the CPU and apply it to wired traffic:

```
(Cisco Controller) > config acl cpu acl01 wired
```

Related Commands

show acl cpu

config acl delete

To delete an access control list (ACL), use the **config acl delete** command.

config acl delete *rule_name*

Syntax Description

rule_name	ACL name that contains up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to delete an ACL named acl101 on the CPU:

```
(Cisco Controller) > config acl delete acl01
```

Related Commands

show acl

config acl layer2

To configure a Layer 2 access control list (ACL), use the **config acl layer2** command.

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*}}

Syntax Description

apply	Applies a Layer 2 ACL to the data path.
acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
create	Creates a Layer 2 ACL.
delete	Deletes a Layer 2 ACL.
rule	Configures a Layer 2 ACL rule.
action	Configures the action for the Layer 2 ACL rule.
index	Index of the Layer 2 ACL rule.
permit	Permits rule action.
deny	Denies rule action.
add	Creates a Layer 2 ACL rule.
change index	Changes the index of the Layer 2 ACL rule.
old_index	Old index of the Layer 2 ACL rule.
new_index	New index of the Layer 2 ACL rule.
delete	Deletes a Layer 2 ACL rule.
etherType	Configures the EtherType of a Layer 2 ACL rule.
etherType	EtherType of a Layer 2 ACL rule. EtherType is used to indicate the protocol that is encapsulated in the payload of an Ethernet frame. The range is a hexadecimal value from 0x0 to 0xffff.
etherTypeMask	Netmask of the EtherType. The range is a hexadecimal value from 0x0 to 0xffff.
swap index	Swaps the index values of two rules.
index1 index2	Index values of two Layer 2 ACL rules.

Command Default

The controller does not have any Layer2 ACLs.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can create a maximum of 16 rules for a Layer 2 ACL.

You can create a maximum of 64 Layer 2 ACLs on a controller.

A maximum of 16 Layer 2 ACLs are supported per access point because an access point supports a maximum of 16 WLANs.

Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an access point does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to apply a Layer 2 ACL:

```
(Cisco Controller) >config acl layer2 apply acl_l2_1
```

config acl rule

To configure ACL rules, use the **config acl rule** command.

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*}

Syntax Description

action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
destination port range	Configure a rule's destination port range.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.

dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule's DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN pre-authentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an ACL to permit access:

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

Related Commands

show acl

config acl url-acl

To configure URL Access Control Lists, use the **config acl url-acl** command.

config acl url-acl [**apply** | **create** | **delete** | **disable** | **enable** | **rule**]
config acl url-aclapply *acl-name*
config acl url-acl create *acl-name*
config acl url-acl delete *acl-name*
config acl url-acldisable
config acl url-aclenable
config acl url-aclrule [**action** | **add** | **delete** | **url**]
config acl url-aclrule action *acl-name index* {**permit** | **deny**}
config acl url-aclrule add *acl-name index*
config acl url-aclrule delete *acl-name index*
config acl url-aclrule url *acl-name index url-name*

Syntax Description

apply *acl-name*	Enter URL ACL name up to 32 alphanumeric charact
create	Create a new URL ACL.
delete	Delete URL ACL.
disable	Disable URL ACL feature.
enable	Enable URL ACL feature.
rule (**action**) (*acl-name*) (*index*)	Configures a rule's action in the URL ACL to either p contains up to 32 alphanumeric characters and URL A
{**permit** | **deny**}	Permit or deny the url rule.
add *acl-name index*	Adds a new rule and rule index.
delete *acl-name index*	Deletes a rule and rule index.
url *acl-name index url-name*	Configures a rule's url address. Enter a url address an

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to create a new URL ACL:

```
(Cisco Controller) >config acl url-acl create test
```

config acl url-acl apply

To apply a URL ACL to a data path, use the **config acl url-acl apply** command.

config acl url-acl apply

Syntax Description

apply	Applies URL ACL to the data path.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to apply a URL ACL to a data path:

```
(Cisco Controller) >config acl url-acl apply
```

config acl url-acl external-server-ip

To redirect the user to a page which will be served when the requested URL is blocked. To configure the external server IP address, use the **config acl url-acl external-server-ip** command.

config acl url-acl external-server-ip *ip-address*

Syntax Description

external-server-ip	Specifies the ACL name.
ip-address	Enter IP address of the external server.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to configure the external server IP address to redirect and show a page when the URL is blocked:

```
(Cisco Controller) > config acl url-acl external-server-ip 192.0.2.1
```

config acl url-acl list-type

To permit or deny traffic for rules in an given acl, use the **config acl url-acl list-type** command.

config acl url-acl list-type *acl_name*{**blacklist** | **whitelist**}

Syntax Description

list-type	Configure list-type for an URL ACL
blacklist	All the rules will have action as deny.
whitelist	All the rules will have action as permit.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to permit traffic for an ACL:

```
(Cisco Controller) > config acl url-acl list-type testacl whitelist
```

config acl url-domain

To add or delete an URL domain for the access control list, use the **config acl url-domain** command.

config acl url-domain {**add** | **delete**} *domain_name acl_name*

Syntax Description

domain_name	URL domain name for the access control list
acl_name	Name of the access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to add a new URL domain for the access control list:

```
(Cisco Controller) > config acl url-domain add cisco.com android
```

The following example shows how to delete an existing URL domain from the access control list:

```
(Cisco Controller) > config acl url-domain delete play.google.com android
```

config advanced 802.11 7920VSIEConfig

To configure the Cisco unified wireless IP phone 7920 VISE parameters, use the **config advanced 802.11 7920VSIEConfig** command.

config advanced 802.11 {**a** | **b**} **7920VSIEConfig** {**call-admission-limit** *limit* | **G711-CU-Quantum** *quantum*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
call-admission-limit	Configures the call admission limit for the 7920s.
G711-CU-Quantum	Configures the value supplied by the infrastructure indicating the current number of channel utilization units that would be used by a single G.711-20ms call.
limit	Call admission limit (from 0 to 255). The default value is 105.
quantum	G711 quantum value. The default value is 15.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to configure the call admission limit for 7920 VISE parameters:

```
(Cisco Controller) >config advanced 802.11 7920VSIEConfig call-admission-limit 4
```

config advanced 802.11 channel add

To add channel to the 802.11 networks auto RF channel list, use the **config advanced 802.11 channel add** command.

config advanced 802.11 {**a** | **b**} **channel add** *channel_number*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a channel to the 802.11 network auto RF channel list.
channel_number	Channel number to add to the 802.11 network auto RF channel list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a channel to the 802.11a network auto RF channel list:

```
(Cisco Controller) >config advanced 802.11 channel add 132
```

config advanced 802.11 channel cleanair-event

To configure CleanAir event driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **config advanced 802.11 channel cleanair-event** command.

config advanced 802.11 {**a** | **b**} **channel cleanair-event** {**enable** | **disable** | **sensitivity** [**low** | **medium** | **high**] | **custom threshold** *threshold_value*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the CleanAir event-driven RRM parameters.
disable	Disables the CleanAir event-driven RRM parameters.
sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
low	(Optional) Specifies low sensitivity.
medium	(Optional) Specifies medium sensitivity
high	(Optional) Specifies high sensitivity
custom	Specifies custom sensitivity.
threshold	Specifies the EDRRM AQ threshold value.
threshold_value	Number of custom threshold.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the CleanAir event-driven RRM parameters:

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event enable
```

The following example shows how to configure high sensitivity for CleanAir event-driven RRM:

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event sensitivity high
```

config advanced 802.11 channel dca anchor-time

To specify the time of day when the Dynamic Channel Assignment (DCA) algorithm is to start, use the **config advanced 802.11 channel dca anchor-time** command.

config advanced 802.11 {**a** | **b**} **channel dca anchor-time** *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
value	Hour of the time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the time of delay when the DCA algorithm starts:

```
(Cisco Controller) > config advanced 802.11 channel dca anchor-time 17
```

Related Commands

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

To configure the Dynamic Channel Assignment (DCA) channel width for all 802.11n radios in the 5-GHz band, use the **config advanced 802.11 channel dca chan-width-11n** command.

config advanced 802.11 {**a** | **b**} **channel dca chan-width-11n** {**20** | **40** | **80**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
20	Sets the channel width for 802.11n radios to 20 MHz.
40	Sets the channel width for 802.11n radios to 40 MHz.
80	Sets the channel width for 802.11ac radios to 80-MHz.

Command Default

The default channel width is 20.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you choose 40, be sure to set at least two adjacent channels in the **config advanced 802.11 channel** {**add** | **delete**} *channel_number* command (for example, a primary channel of 36 and an extension channel of 40). If you set only one channel, that channel is not used for the 40-MHz channel width.

To override the globally configured DCA channel width setting, you can statically configure an access point's radio for 20- or 40-MHz mode using the **config 802.11 chan_width** command. If you then change the static configuration to global on the access point radio, the global DCA configuration overrides the channel width configuration that the access point was previously using.

The following example shows how to add a channel to the 802.11a network auto channel list:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 40
```

The following example shows how to set the channel width for the 802.11ac radio as 80-MHz:

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 80
```

config advanced 802.11 channel dca interval

To specify how often the Dynamic Channel Assignment (DCA) is allowed to run, use the **config advanced 802.11 channel dca interval** command.

config advanced 802.11 {**a** | **b**} **channel dca interval** *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
value	Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds).

Command Default

The default DCA channel interval is 10 (10 minutes).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If your controller supports only OfficeExtend access points, we recommend that you set the DCA interval to 6 hours for optimal performance. For deployments with a combination of OfficeExtend access points and local access points, the range of 10 minutes to 24 hours can be used.

The following example shows how often the DCA algorithm is allowed to run:

```
(Cisco Controller) > config advanced 802.11 channel dca interval 8
```

Related Commands

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

To configure the 5-GHz minimum RSSI energy metric for DCA, use the **config advanced 802.11 channel dca min-metric** command.

config advanced 802.11 {**a** | **b**} **channel dca** *RSSI_value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
RSSI_value	Minimum received signal strength indicator (RSSI) that is required for the DCA to trigger a channel change. The range is from –100 to –60 dBm.

Command Default

The default minimum RSSI energy metric for DCA is –95 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the minimum 5-GHz RSSI energy metric for DCA:

```
(Cisco Controller) > config advanced 802.11a channel dca min-metric -80
```

In the above example, the RRM must detect an interference energy of at least -80 dBm in RSSI for the DCA to trigger a channel change.

Related Commands

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

To specify how sensitive the Dynamic Channel Assignment (DCA) algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels, use the **config advanced 802.11 channel dca sensitivity** command.

config advanced 802.11 {**a** | **b**} **channel dcasensitivity** {**low** | **medium** | **high**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
low	Specifies the DCA algorithm is not particularly sensitive to environmental changes. See the "Usage Guidelines" section for more information.
medium	Specifies the DCA algorithm is moderately sensitive to environmental changes. See the "Usage Guidelines" section for more information.
high	Specifies the DCA algorithm is highly sensitive to environmental changes. See the "Usage Guidelines" section for more information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The DCA sensitivity thresholds vary by radio band as shown in the table below.

To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

Table 4: DCA Sensitivity Thresholds

Sensitivity	2.4-GHz DCA Sensitivity Threshold	5-GHz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

The following example shows how to configure the value of DCA algorithm's sensitivity to low:

```
(Cisco Controller) > config advanced 802.11 channel dca sensitivity low
```

Related Commands

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel foreign

To have Radio Resource Management (RRM) consider or ignore foreign 802.11a interference avoidance in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel foreign** command.

config advanced 802.11 {**a** | **b**} **channel foreign** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the foreign access point 802.11a interference avoidance in the channel assignment.
disable	Disables the foreign access point 802.11a interference avoidance in the channel assignment.

Command Default

The default value for the foreign access point 802.11a interference avoidance in the channel assignment is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to have RRM consider foreign 802.11a interference when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11a channel foreign enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel foreign

config advanced 802.11 channel load

To have Radio Resource Management (RRM) consider or ignore the traffic load in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel load** command.

config advanced 802.11 {**a** | **b**} **channel load** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.
disable	Disables the Cisco lightweight access point 802.11a load avoidance in the channel assignment.

Command Default

The default value for Cisco lightweight access point 802.11a load avoidance in the channel assignment is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to have RRM consider the traffic load when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel load enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel load

config advanced 802.11 channel noise

To have Radio Resource Management (RRM) consider or ignore non-802.11a noise in making channel selection updates for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel noise** command.

config advanced 802.11 {**a** | **b**} **channel noise** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables non-802.11a noise avoidance in the channel assignment. or ignore.
disable	Disables the non-802.11a noise avoidance in the channel assignment.

Command Default

The default value for non-802.11a noise avoidance in the channel assignment is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to have RRM consider non-802.11a noise when making channel selection updates for all 802.11a Cisco lightweight access points:

```
(Cisco Controller) > config advanced 802.11 channel noise enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel outdoor-ap-dca

To enable or disable the controller to avoid checking the non-Dynamic Frequency Selection (DFS) channels, use the **config advanced 802.11 channel outdoor-ap-dca** command.

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables 802.11 network DCA list option for outdoor access point.
disable	Disables 802.11 network DCA list option for outdoor access point.

Command Default

The default value for 802.11 network DCA list option for outdoor access point is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The **config advanced 802.11** {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**} command is applicable only for deployments having outdoor access points such as 1522 and 1524.

The following example shows how to enable the 802.11a DCA list option for outdoor access point:

```
(Cisco Controller) > config advanced 802.11a channel outdoor-ap-dca enable
```

Related Commands

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel pda-prop

To enable or disable propagation of persistent devices, use the **config advanced 802.11 channel pda-prop** command.

config advanced 802.11 {**a** | **b**} **channel pda-prop** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the 802.11 network DCA list option for the outdoor access point.
disable	Disables the 802.11 network DCA list option for the outdoor access point.

Command Default

The default 802.11 network DCA list option for the outdoor access point is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable or disable propagation of persistent devices:

```
(Cisco Controller) > config advanced 802.11 channel pda-prop enable
```

config advanced 802.11 channel update

To have Radio Resource Management (RRM) initiate a channel selection update for all 802.11a Cisco lightweight access points, use the **config advanced 802.11 channel update** command.

config advanced 802.11 {**a** | **b**} **channel update**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate a channel selection update for all 802.11a network access points:

```
(Cisco Controller) > config advanced 802.11a channel update
```

config advanced 802.11 coverage

To enable or disable coverage hole detection, use the **config advanced 802.11 coverage** command.

config advanced 802.11 { **a** | **b** } **coverage** { **enable** | **disable** }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the coverage hole detection.
disable	Disables the coverage hole detection.

Command Default

The default coverage hole detection value is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you enable coverage hole detection, the controller automatically determines, based on data that is received from the access points, whether any access points have clients that are potentially located in areas with poor coverage.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to enable coverage hole detection on an 802.11a network:

```
(Cisco Controller) > config advanced 802.11a coverage enable
```

Related Commands

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

To specify the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point, use the **config advanced 802.11 coverage exception global** command.

config advanced 802.11 {**a** | **b**} **coverage exception global** *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
percent	Percentage of clients. Valid values are from 0 to 100%.

Command Default

The default percentage value for clients on an access point is 25%.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the**config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to specify the percentage of clients for all 802.11a access points that are experiencing a low signal level:

```
(Cisco Controller) > config advanced 802.11 coverage exception global 50
```

Related Commands

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

To specify the failure rate threshold for uplink data or voice packets, use the **config advanced 802.11 coverage fail-rate** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **fail-rate** *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
percent	Failure rate as a percentage. Valid values are from 1 to 100 percent.

Command Default

The default failure rate threshold uplink coverage fail-rate value is 20%.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the**config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the threshold count for minimum uplink failures for data packets:

```
(Cisco Controller) > config advanced 802.11 coverage fail-rate 80
```

Related Commands

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

To specify the minimum number of clients on an access point with an received signal strength indication (RSSI) value at or below the data or voice RSSI threshold, use the **config advanced 802.11 coverage level global** command.

config advanced 802.11 {**a** | **b**} **coverage level global** *clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
clients	Minimum number of clients. Valid values are from 1 to 75.

Command Default

The default minimum number of clients on an access point is 3.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to specify the minimum number of clients on all 802.11a access points with an RSSI value at or below the RSSI threshold:

```
(Cisco Controller) > config advanced 802.11 coverage level global 60
```

Related Commands

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

To specify the minimum failure count threshold for uplink data or voice packets, use the **config advanced 802.11 coverage packet-count** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **packet-count** *packets*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
packets	Minimum number of packets. Valid values are from 1 to 255 packets.

Command Default

The default failure count threshold for uplink data or voice packets is10.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the failure count threshold for uplink data packets:

```
(Cisco Controller) > config advanced 802.11 coverage packet-count 100
```

Related Commands

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

To specify the minimum receive signal strength indication (RSSI) value for packets that are received by an access point, use the **config advanced 802.11 coverage rssi-threshold** command.

config advanced 802.11 {**a** | **b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
data	Specifies the threshold for data packets.
voice	Specifies the threshold for voice packets.
rssi	Valid values are from –60 to –90 dBm.

Command Default

- The default RSSI value for data packets is –80 dBm.
- The default RSSI value for voice packets is –75 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The *rssi* value that you enter is used to identify coverage holes (or areas of poor coverage) within your network. If the access point receives a packet in the data or voice queue with an RSSI value that is below the value that you enter, a potential coverage hole has been detected.

The access point takes RSSI measurements every 5 seconds and reports them to the controller in 90-second intervals.

If both the number and percentage of failed packets exceed the values that you entered in the **config advanced 802.11 coverage packet-count** and **config advanced 802.11 coverage fail-rate** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The controller uses this information to distinguish between real and false coverage holes and excludes clients with poor roaming logic. A coverage hole is detected if both the number and percentage of failed clients meet or exceed the values entered in the **config advanced 802.11 coverage level global** and **config advanced 802.11 coverage exception global** commands over a 90-second period. The controller determines whether the coverage hole can be corrected and, if appropriate, mitigates the coverage hole by increasing the transmit power level for that specific access point.

The following example shows how to configure the minimum receive signal strength indication threshold value for data packets that are received by an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11a coverage rssi-threshold -60
```

Related Commands

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

To enable a specific Enhanced Distributed Channel Access (EDCA) profile on a 802.11a network, use the **config advanced 802.11 edca-parameters** command.

config advanced 802.11 { **a** | **b** } **edca-parameters** { **wmm-default** | **svp-voice** | **optimized-voice** | **optimized-video-voice** | **custom-voice** | **fastlane** | **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)* } }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option if voice or video services are not deployed on your network.
svp-voice	Enables Spectralink voice-priority parameters. Choose this option if Spectralink phones are deployed on your network to improve the quality of calls.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option if voice services other than Spectralink are deployed on your network.
optimized-video-voice	Enables EDCA voice-optimized and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network. **Note** If you deploy video services, admission control must be disabled.
custom-voice	Enables custom voice EDCA parameters for 802.11a. The EDCA parameters under this option also match the 6.0 WMM EDCA parameters when this profile is applied.
fastlane	Enables fastlane on compatible devices.

custom-set	Enables customization of EDCA parameters • **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 Profile Name - Enter the QoS profile name: • bronze • silver • gold • platinum

Command Default

The default EDCA parameter is **wmm-default**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2.110.0	In this release, custom-set keyword was added to edca-parameters command.
8.3	This command was modified and the **fastlane** keyword was added.

Examples

The following example shows how to enable Spectralink voice-priority parameters:

```
(Cisco Controller) > config advanced 802.11 edca-parameters svp-voice
```

Related Commands

config advanced 802.11b edca-parameters	Enables a specific Enhanced Distributed Channel Access (EDCA) profile on the 802.11a network.
show 802.11a	Displays basic 802.11a network settings.

config advanced 802.11 factory

To reset 802.11a advanced settings back to the factory defaults, use the **config advanced 802.11 factory** command.

config advanced 802.11 {**a** | **b**} **factory**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to return all the 802.11a advanced settings to their factory defaults:

```
(Cisco Controller) > config advanced 802.11a factory
```

Related Commands

show advanced 802.11a channel

config advanced 802.11 group-member

To configure members in 802.11 static RF group, use the **config advanced 802.11 group-member** command.

config advanced 802.11 {**a** | **b**} **group-member** {**add** | **remove**} *controller controller-ip-address*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
add	Adds a controller to the static RF group.
remove	Removes a controller from the static RF group.
controller	Name of the controller to be added.
controller-ip-address	IP address of the controller to be added.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a controller in the 802.11a automatic RF group:

```
(Cisco Controller) > config advanced 802.11a group-member add cisco-controller 209.165.200.225
```

Related Commands

show advanced 802.11a group

config advanced 802.11 group-mode

config advanced 802.11 group-mode

To set the 802.11a automatic RF group selection mode on or off, use the **config advanced 802.11 group-mode** command.

config advanced 802.11 {**a** | **b**} **group-mode** {**auto** | **leader** | **off** | **restart**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
auto	Sets the 802.11a RF group selection to automatic update mode.
leader	Sets the 802.11a RF group selection to static mode, and sets this controller as the group leader.
off	Sets the 802.11a RF group selection to off.
restart	Restarts the 802.11a RF group selection.

Command Default

The default 802.11a automatic RF group selection mode is auto.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the 802.11a automatic RF group selection mode on:

```
(Cisco Controller) > config advanced 802.11a group-mode auto
```

The following example shows how to configure the 802.11a automatic RF group selection mode off:

```
(Cisco Controller) > config advanced 802.11a group-mode off
```

Related Commands

show advanced 802.11a group

config advanced 802.11 group-member

config advanced 802.11 logging channel

To turn the channel change logging mode on or off, use the **config advanced 802.11 logging channel** command.

config advanced 802.11 {**a** | **b**} **logging channel** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
logging channel	Logs channel changes.
on	Enables the 802.11 channel logging.
off	Disables 802.11 channel logging.

Command Default

The default channel change logging mode is Off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a logging channel selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging channel on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging channel

config advanced 802.11 logging coverage

To turn the coverage profile logging mode on or off, use the **config advanced 802.11 logging coverage** command.

config advanced 802.11 {**a** | **b**} **logging coverage** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 coverage profile violation logging.
off	Disables the 802.11 coverage profile violation logging.

Command Default

The default coverage profile logging mode is Off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a coverage profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging coverage on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging coverage

config advanced 802.11 logging foreign

To turn the foreign interference profile logging mode on or off, use the **config advanced 802.11 logging foreign** command.

config advanced 802.11 {**a** | **b**} **logging foreign** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 foreign interference profile violation logging.
off	Disables the 802.11 foreign interference profile violation logging.

Command Default

The default foreign interference profile logging mode is Off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a foreign interference profile violation logging selection mode on:

```
(Cisco Controller) > config advanced 802.11a logging foreign on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging foreign

config advanced 802.11 logging load

To turn the 802.11a load profile logging mode on or off, use the **config advanced 802.11 logging load** command.

config advanced 802.11 {**a** | **b**} **logging load** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 load profile violation logging.
off	Disables the 802.11 load profile violation logging.

Command Default

The default 802.11a load profile logging mode is Off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a load profile logging mode on:

```
(Cisco Controller) > config advanced 802.11 logging load on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging load

config advanced 802.11 logging noise

To turn the 802.11a noise profile logging mode on or off, use the **config advanced 802.11 logging noise** command.

config advanced 802.11 {**a** | **b**} **logging noise** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 noise profile violation logging.
off	Disables the 802.11 noise profile violation logging.

Command Default

The default 802.11a noise profile logging mode is off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a noise profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging noise on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging noise

config advanced 802.11 logging performance

To turn the 802.11a performance profile logging mode on or off, use the **config advanced 802.11 logging performance** command.

config advanced 802.11 {**a** | **b**} **logging performance** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 performance profile violation logging.
off	Disables the 802.11 performance profile violation logging.

Command Default

The default 802.11a performance profile logging mode is off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a performance profile logging mode on:

```
(Cisco Controller) > config advanced 802.11a logging performance on
```

Related Commands

show advanced 802.11a logging

config advanced 802.11b logging performance

config advanced 802.11 logging txpower

To turn the 802.11a transmit power change logging mode on or off, use the **config advanced 802.11 logging txpower** command.

config advanced 802.11 {**a** | **b**} **logging txpower** {**on** | **off**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
on	Enables the 802.11 transmit power change logging.
off	Disables the 802.11 transmit power change logging.

Command Default

The default 802.11a transmit power change logging mode is off (disabled).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn the 802.11a transmit power change mode on:

```
(Cisco Controller) > config advanced 802.11 logging txpower off
```

Related Commands

show advanced 802.11 logging

config advanced 802.11b logging power

config advanced 802.11 monitor channel-list

To set the 802.11a noise, interference, and rogue monitoring channel list, use the **config advanced 802.11 monitor channel-list** command.

config advanced 802.11 {**a** | **b**} **monitor channel-list** {**all** | **country** | **dca**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
all	Monitors all channels.
country	Monitors the channels used in the configured country code.
dca	Monitors the channels used by the automatic channel assignment.

Command Default

The default 802.11a noise, interference, and rogue monitoring channel list is country.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to monitor the channels used in the configured country:

```
(Cisco Controller) > config advanced 802.11 monitor channel-list country
```

Related Commands

show advanced 802.11a monitor coverage

config advanced 802.11 monitor load

To set the load measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor load** command.

config advanced 802.11 {**a** | **b**} **monitor load** *seconds*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
seconds	Load measurement interval between 60 and 3600 seconds.

Command Default

The default load measurement interval is 60 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the load measurement interval to 60 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor load 60
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor load

config advanced 802.11 monitor measurement

To set the signal measurement interval between 60 and 3600 seconds, use the **config advanced 802.11 monitor measurement** command.

config advanced 802.11 {**a** | **b**} **monitor measurement** *seconds*

Syntax Description

seconds	Signal measurement interval that you need to enter. Valid range is between 60 and 3600 seconds.

Command Default

The default signal measurement interval is 180 seconds.

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to set the signal measurement interval to 300 seconds:

```
(Cisco Controller) > config advanced 802.11 monitor measurement 300
```

config advanced 802.11 monitor mode

To enable or disable 802.11a access point monitoring, use the **config advanced 802.11 monitor mode** command.

config advanced 802.11 {**a** | **b**} **monitor mode** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
enable	Enables the 802.11 access point monitoring.
disable	Disables the 802.11 access point monitoring.

Command Default

The default 802.11a access point monitoring is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the 802.11a access point monitoring:

```
(Cisco Controller) > config advanced 802.11a monitor mode enable
```

Related Commands

show advanced 802.11a monitor

config advanced 802.11b monitor mode

config advanced 802.11 monitor ndp-type

To configure the 802.11 access point radio resource management (RRM) Neighbor Discovery Protocol (NDP) type, use the **config advanced 802.11 monitor ndp-type** command:

config advanced 802.11 {**a** | **b**} **monitor ndp-type** {**protected** | **transparent**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
protected	Specifies the Tx RRM protected NDP.
transparent	Specifies the Tx RRM transparent NDP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you configure the 802.11 access point RRM NDP type, ensure that you have disabled the network by entering the **config 802.11 disable network** command.

The following example shows how to enable the 802.11a access point RRM NDP type as protected:

```
(Cisco Controller) > config advanced 802.11 monitor ndp-type protected
```

Related Commands

config advanced 802.11 monitor

config advanced 802.11 monitor mode

config advanced 802.11 disable

config advanced 802.11 monitor timeout-factor

To configure the 802.11 neighbor timeout factor, use the **config advanced 802.11 monitor timeout-factor** command:

config advanced 802.11 {**a** | **b**} **monitor timeout-factor** *factor-value-in-minutes*

Syntax Description

factor-value-in-minutes	Neighbor timeout factor value that you must enter. Valid range is between 5 minutes to 60 minutes. We recommend that you set the timeout factor to 60 minutes.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced

Usage Guidelines

If you are using Release 8.1 or a later release, we recommend that you set the timeout factor to 60 minutes. If the access point radio does not receive a neighbor packet from an existing neighbor within 60 minutes, the controller deletes the neighbor from the neighbor list.

Note The Neighbor Timeout Factor was hardcoded to 60 minutes in Release 7.6, but was changed to 5 minutes in Release 8.0.100.0.

config advanced 802.11 optimized roaming

To configure the optimized roaming parameters for each 802.11 band, use the **config advanced 802.11 optimized roaming** command.

config advanced {**802.11a** | **802.11b**} **optimized-roaming** {**enable** | **disable** | **interval** *seconds* | **datarate** *mbps*}

Syntax Description

802.11a	Configures optimized roaming parameters for 802.11a network.
802.11b	Configures optimized roaming parameters for 802.11b network.
enable	Enables optimized roaming.
disable	Disables optimized roaming.
interval	Configures the client coverage reporting interval for 802.11a/b networks.
seconds	Client coverage reporting interval in seconds. The range is from 5 to 90 seconds.
datarate	Configures the threshold data rate for 802.11a/b networks.
mbps	Threshold data rate in Mbps for 802.11a/b networks. For 802.11a, the configurable data rates are 6, 9, 12, 18, 24, 36, 48, and 54. For 802.11b, the configurable data rates are 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, and 54. You can configure 0 to disable the data rate for disassociating clients.

Command Default

By default, optimized roaming is disabled. The default value for client coverage reporting interval is 90 seconds and threshold data rate is 0 (disabled state).

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

You must disable the 802.11a/b network before you configure the optimized roaming reporting interval. If you configure a low value for the reporting interval, the network can get overloaded with coverage report messages.

The following example shows how to enable optimized roaming for the 802.11a network:

```
(Cisco Controller) > config advanced 802.11a optimized roaming enable
```

The following example shows how to configure the data rate interval for the 802.11a network:

```
(Cisco Controller) > config advanced 802.11a optimized roaming datarate 9
```

config advanced 802.11 packet

To configure the maximum packet retries, consecutive packet failure thresholds, and the default timeout value, use **config advanced 802.11 packet** command.

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)*> }

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
QoS Profile Name	• bronze • silver • gold • platinum
max-client-count	Configures the consecutive packet failure threshold before disassociating a client. *threshold value* - Enter the client count threshold value in the range 0 to 1000
max-packet-count	Configures the consecutive packet failure threshold before not retrying failure packet. *threshold value* - Enter the packet failure threshold value in the range 0 to 1000
max-retry	Configures the packet retry time for failure packet. *maximum retry count* - Enter the maximum number of retries allowed.
timeout	Configures the packet aging or discard timeout threshold. *time* - Enter the maximum time before the packet times out.

Command Default

The default values for parameters in **config advanced 802.11 packet** command are:

Keyword	Default Value
max-client-count	500
max-packet-count	100
max-retry	3

Keyword	Default Value
timeout	35 miliseconds

Command History

Release	Modification
8.2	packet command was introduced in this release.

```
(Cisco Controller) > config advanced 802.11a packet platinum max-packet-count 200
```

Related Commands

show 802.11a	Displays basic 802.11a network settings.

config advanced 802.11 profile clients

To set the Cisco lightweight access point clients threshold between 1 and 75 clients, use the **config advanced 802.11 profile clients** command.

config advanced 802.11 {**a** | **b**} **profile clients** {**global** | *cisco_ap*} *clients*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
clients	802.11a Cisco lightweight access point client threshold between 1 and 75 clients.

Command Default

The default Cisco lightweight access point clients threshold is 12 clients.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set all Cisco lightweight access point clients thresholds to 25 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients global 25
Global client count profile set.
```

The following example shows how to set the AP1 clients threshold to 75 clients:

```
(Cisco Controller) >config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

config advanced 802.11 profile customize

To turn customizing on or off for an 802.11a Cisco lightweight access point performance profile, use the **config advanced 802.11 profile customize** command.

config advanced 802.11 {**a** | **b**} **profile customize** *cisco_ap* {**on** | **off**}

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
cisco_ap	Cisco lightweight access point.
on	Customizes performance profiles for this Cisco lightweight access point.
off	Uses global default performance profiles for this Cisco lightweight access point.

Command Default

The default state of performance profile customization is Off.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
(Cisco Controller) >config advanced 802.11 profile customize AP1 on
```

config advanced 802.11 profile foreign

To set the foreign 802.11a transmitter interference threshold between 0 and 100 percent, use the **config advanced 802.11 profile foreign** command.

config advanced 802.11 {**a** | **b**} **profile foreign** {**global** | *cisco_ap*} *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access points.
cisco_ap	Cisco lightweight access point name.
percent	802.11a foreign 802.11a interference threshold between 0 and 100 percent.

Command Default

The default foreign 802.11a transmitter interference threshold value is 10.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the foreign 802.11a transmitter interference threshold for all Cisco lightweight access points to 50 percent:

```
(Cisco Controller) >config advanced 802.11a profile foreign global 50
```

The following example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile foreign AP1 0
```

config advanced 802.11 profile noise

To set the 802.11a foreign noise threshold between –127 and 0 dBm, use the **config advanced 802.11 profile noise** command.

config advanced 802.11 {**a** | **b**} **profile noise** {**global** | *cisco_ap*} *dBm*

Syntax Description

a	Specifies the 802.11a/n network.
b	Specifies the 802.11b/g/n network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
dBm	802.11a foreign noise threshold between –127 and 0 dBm.

Command Default

The default foreign noise threshold value is –70 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the 802.11a foreign noise threshold for all Cisco lightweight access points to –127 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise global -127
```

The following example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
(Cisco Controller) >config advanced 802.11a profile noise AP1 0
```

config advanced 802.11 profile throughput

To set the Cisco lightweight access point data-rate throughput threshold between 1000 and 10000000 bytes per second, use the **config advanced 802.11 profile throughput** command.

config advanced 802.11 {**a** | **b**} **profile throughput** {**global** | *cisco_ap*} *value*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures all 802.11a Cisco lightweight access point specific profiles.
cisco_ap	Cisco lightweight access point name.
value	802.11a Cisco lightweight access point throughput threshold between 1000 and 10000000 bytes per second.

Command Default

The default Cisco lightweight access point data-rate throughput threshold value is 1,000,000 bytes per second.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set all Cisco lightweight access point data-rate thresholds to 1000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput global 1000
```

The following example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
(Cisco Controller) >config advanced 802.11 profile throughput AP1 10000000
```

config advanced 802.11 profile utilization

To set the RF utilization threshold between 0 and 100 percent, use the **config advanced 802.11 profile utilization** command. The operating system generates a trap when this threshold is exceeded.

config advanced 802.11 {**a** | **b**} **profile utilization** {**global** | *cisco_ap*} *percent*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Configures a global Cisco lightweight access point specific profile.
cisco_ap	Cisco lightweight access point name.
percent	802.11a RF utilization threshold between 0 and 100 percent.

Command Default

The default RF utilization threshold value is 80 percent.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the RF utilization threshold for all Cisco lightweight access points to 0 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization global 0
```

The following example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
(Cisco Controller) >config advanced 802.11 profile utilization AP1 100
```

config advanced 802.11 receiver

To set the advanced receiver configuration settings, use the **config advanced 802.11 receiver** command.

config advanced 802.11 {**a** | **b**} **receiver** {**default** | **rxstart jumpThreshold** *value*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
receiver	Specifies the receiver configuration.
default	Specifies the default advanced receiver configuration.
rxstart jumpThreshold	Specifies the receiver start signal. **Note** We recommend that you do not use this option as it is for Cisco internal use only.
value	Jump threshold configuration value between 0 and 127.

Command Default

None

Usage Guidelines

- Before you change the 802.11 receiver configuration, you must disable the 802.11 network.
- We recommend that you do not use the **rxstart jumpThreshold** *value* option as it is for Cisco internal use only.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent changes to receiver parameters while the network is enabled:

```
(Cisco Controller) > config advanced 802.11 receiver default
```

config advanced 802.11 reporting measurement

To set the reporting measurement interval between 60 and 3600 seconds,, use the **config advanced 802.11 reporting measurement** command.

config advanced 802.11 {**a** | **b**} **reporting measurement** *seconds*

Syntax Description

seconds	Reporting measurement interval that you need to enter. Valid range is between 60 and 3600 seconds.

Command Default

The default reporting measurement interval is 180 seconds.

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to set the signal measurement interval to 300 seconds:

```
(Cisco Controller) > config advanced 802.11 reporting measurement 300
```

config advanced 802.11 tpc-version

To configure the Transmit Power Control (TPC) version for a radio, use the **config advanced 802.11 tpc-version** command.

config advanced 802.11{**a** | **b**} **tpc-version** {**1** | **2**}

Syntax Description

1	Specifies the TPC version 1 that offers strong signal coverage and stability.
2	Specifies TPC version 2 is for scenarios where voice calls are extensively used. The Tx power is dynamically adjusted with the goal of minimum interference. It is suitable for dense networks. In this mode, there could be higher roaming delays and coverage hole incidents.

Command Default

The default TPC version for a radio is 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the TPC version as 1 for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpc-version 1
```

Related Commands

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv1-thresh

To configure the threshold for Transmit Power Control (TPC) version 1 of a radio, use the **config advanced 802.11 tpcv1-thresh** command.

config advanced 802.11 {**a** | **b**} **tpcv1-thresh** *threshold*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g/n network.
threshold	Threshold value between –50 dBm to –80 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold as –60 dBm for TPC version 1 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv1-thresh -60
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

To configure the computational intensity for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-intense** command.

config advanced 802.11{**a** | **b**} **tpcv2-intense** *intensity*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g/n network.
intensity	Computational intensity value between 1 to 100.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the computational intensity as 50 for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-intense 50
```

Related Commands

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

To configure the Transmit Power Control Version 2 on a per-channel basis, use the **config advanced 802.11 tpcv2-per-chan** command.

config advanced 802.11 {**a** | **b**} **tpcv2-per-chan** {**enable** | **disable**}

Syntax Description

enable	Enables the configuration of TPC version 2 on a per-channel basis.
disable	Disables the configuration of TPC version 2 on a per-channel basis.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable TPC version 2 on a per-channel basis for the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11 tpcv2-per-chan enable
```

Related Commands

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

config advanced 802.11 tpcv2-thresh

To configure the threshold for Transmit Power Control (TPC) version 2 of a radio, use the **config advanced 802.11 tpcv2-thresh** command.

config advanced 802.11{**a** | **b**} **tpcv2-thresh** *threshold*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
threshold	Threshold value between –50 dBm to –80 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold as –60 dBm for TPC version 2 of the 802.11a radio:

```
(Cisco Controller) > config advanced 802.11a tpcv2-thresh -60
```

Related Commands

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

To initiate updates of the 802.11a transmit power for every Cisco lightweight access point, use the **config advanced 802.11 txpower-update** command.

config advanced 802.11 {**a** | **b**} **txpower-update**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate updates of 802.11a transmit power for an 802.11a access point:

```
(Cisco Controller) > config advanced 802.11 txpower-update
```

Related Commands

config advance 802.11b txpower-update

config advanced eap

To configure advanced extensible authentication protocol (EAP) settings, use the **config advanced eap** command.

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*} | **rsn-capability-validation** {**enable** | **disable** }}

Syntax Description

bcast-key-interval *seconds*	Specifies the EAP-broadcast key renew interval time in seconds. The range is from 120 to 86400 seconds.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller waits before retransmitting an EAPOL (WPA) key message to a wireless client using EAP or WPA/WPA-2 PSK. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting an EAP Identity Request message to a wireless client. The default value is 30 seconds.
identity-request- retries	Specifies the maximum number of times (0 to 4 retries) that the controller retransmits an EAPOL (WPA) key message to a wireless client. The default value is 2.
key-index *index*	Specifies the key index (0 or 3) used for dynamic wired equivalent privacy (WEP).
max-login-ignore- identity-response	When enabled, this command ignores the limit set for the number of devices that can be connected to the controller with the same username using 802.1xauthentication. When disabled, this command limits the number of devices that can be connected to the controller with the same username. This option is not applicable for Web auth user. Use the command **config netuser maxUserLogin** to set the limit of maximum number of devices per same username

enable	Ignores the same username reaching the maximum EAP identity response.
disable	Checks the same username reaching the maximum EAP identity response.
request-timeout	For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the amount of time (1 to 120 seconds) that the controller waits before retransmitting the message to a wireless client. The default value is 30 seconds.
request-retries	(Optional) For EAP messages other than Identity Requests or EAPOL (WPA) key messages, specifies the maximum number of times (0 to 20 retries) that the controller retransmits the message to a wireless client. The default value is 2.
rsn-capability-validation {**enable** | **disable**}	Allows you to enable or disable RSN-capability (2-Byte in EAPOL-M2 frame) validation with respect to association request.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.5.151.0 8.10	The **rsn-capability-validation** parameter was added.

The following example shows how to configure the key index used for dynamic wired equivalent privacy (WEP):

```
(Cisco Controller) > config advanced eap key-index 0
```

config advanced fra service-priority

To configure the Flexible Radio Assignment (FRA) service priority, use the **config advanced fra service-priority** command.

config advanced fra service-priority [**client-aware** | **coverage** | **service-assurance**]

Syntax Description

client-aware	Configure the FRA service priority to Client Aware.
coverage	Configure the FRA service priority to Coverage.
service-assurance	Configure the FRA service priority to Service Assurance. **service-assurance** is not supported in 8.5 release.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The following example shows how to configure the FRA service priority to client-aware:

```
(Cisco Controller) > config advanced fra service-priority client-aware
```

The following example shows how to configure the FRA service priority to coverage:

```
(Cisco Controller) > config advanced fra service-priority coverage
```

Related Commands

config advanced fra client-aware client-select

config advanced fra client-aware client-reset

config advanced fra client-aware client-select

To configure the utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role, use the **config advanced fra client-aware client-select** command.

config advanced fra client-aware client-select *percent*

Syntax Description

percent	Utilization percentage value ranges from 0 to 100.

Note The **client-select** *percent* value must be greater than the **client-reset** *percent* value. If not, you get to see the following message:

Input for Client Aware FRA Client Reset Utilization Threshold is out of range.

Command Default

The default percent value for client-select is 50%.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The following example shows how to configure the utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) > config advanced fra client-aware client-select 20
```

Related Commands

config advanced fra client-aware client-reset

config advanced fra client-aware client-reset

To configure the utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode, use the **config advanced fra client-aware client-reset** command.

config advanced fra client-aware client-reset *percent*

Syntax Description

percent	Utilization percentage value ranges from 0 to 100.

Note If the **client-reset** *percent* value is greater than the **client-select** *percent* value, you get to see the following message:

Input for Client Aware FRA Client Reset Utilization Threshold is out of range.

Command Default

The default percent value for client-reset is 5%.

Command Modes

Global configuration (config)

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The following example shows how to configure the utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) > config advanced fra client-aware client-reset 15
```

Related Commands

config advanced fra client-aware client-select

config advanced hyperlocation

To configure Cisco Hyperlocation globally on all APs that have the Cisco Hyperlocation module, use the **config advanced hyperlocation** command.

config advanced hyperlocation {**enable** | **disable** | **ntp** *ipv4-addr* | **flag-unset** *ap-name* | **reset-threshold** *value* | **threshold** *value* | **trigger-threshold** *value*}

Syntax Description

enable	Enables Cisco Hyperlocation globally on all Cisco APs that have the Cisco Hyperlocation module.
disable	Disables Cisco Hyperlocation globally on all Cisco APs that have the Cisco Hyperlocation module.
ntp *ipv4-addr*	Sets up the NTP server for Cisco Hyperlocation. Enter the IPv4 address of the NTP server that all APs that are involved in this calculation need to synchronize to.
flag-unset *ap-name*	Configures the AP specified to accept any other level of Cisco Hyperlocation configuration.
reset-threshold *value*	Configures PRL reset threshold value below which RSSI is ignored while sending to controller.
reset-threshold *value*	Configures the threshold value below which RSSI is ignored while sending to controller.
trigger-threshold *value*	Configures the number of scan cycles between PAK RSSI location trigger.

Command Default

Disabled

Usage Guidelines

- Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.
- We recommend that you use the same NTP server that is used by the general controller infrastructure. The scans from multiple AP need to be synchronized for the location to be accurately calculated.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable Cisco Hyperlocation on all APs:

```
(Cisco Controller) >config advanced hyperlocation enable
```

config advanced hyperlocation apgroup

To configure Cisco Hyperlocation for an AP group that contains APs with the Cisco Hyperlocation module, use the **config advanced hyperlocation apgroup** command.

config advanced hyperlocation apgroup *group-name* {**enable** | **disable**}

config advanced hyperlocation apgroup *group-name* **ntp** *server-ipv4-address*

Syntax Description

enable	Enables Cisco Hyperlocation for the AP group that contains APs with the Cisco Hyperlocation module
disable	Disables Cisco Hyperlocation for the AP group that contains APs with the Cisco Hyperlocation module
ntp	Configures NTP server for the AP group.
server-ipv4-address	IPv4 address of the NTP server for the AP group.

Command Default

Disabled

Usage Guidelines

Cisco Hyperlocation in enabled state has an impact on performance where both radios of APs that do not have Cisco Hyperlocation module go off-channel for about 100 milliseconds every 3 seconds.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable Cisco Hyperlocation for an AP group:

```
(Cisco Controller) >config advanced hyperlocation apgroup myapgroup enable
```

config advanced hyperlocation ble-beacon

To configure BLE beacon parameters, use the **config advanced hyperlocation ble-beacon** command.

config advanced hyperlocation ble-beacon {**advertised-power** *rssi-value* | **interval** *value* | **ap-name** *ap-name* | {**advertised-power** *rssi-value* | **interval** *value* | **unset**}}

Syntax Description

advertised-power *rssi-value*	Configures BLE advertised transmit power for all APs. Valid range is between –40 dBm to –100 dBm
interval *value*	Configures BLE beacon interval for all APs. Valid range is between 1 to 10 seconds.
ap-name *ap-name*	Configures BLE beacon parameters for the specified AP.
unset	Clears AP-specific BLE configuration and sets global BLE configuration when applied.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to set the BLE beacon interval for all APs to 8 seconds:

```
(Cisco Controller) >config advanced hyperlocation ble-beacon interval 8
```

config advanced hyperlocation ble-beacon beacon-id

To configure BLE beacon parameters for a specific beacon, use the **config advanced hyperlocation ble-beacon beacon-id** command.

config advanced hyperlocation ble-beacon beacon-id *id* {{**delete** | **enable** | **disable** } | **add** {**txpwr** *value* | **uuid** *value*} | **add ap-group** *group-name* {**enable** | **disable** | **major** *mjr-value* | **minor** *mnr-value* | **txpwr** *value* | **uuid** *value*} | **add ap-name** *ap-name* {**enable** | **disable** | **major** *mjr-value* | **minor** *mnr-value* | **txpwr** *value* | **uuid** *value*}}

Syntax Description

beacon-id *id*	Configures BLE parameters for the beacon ID that you enter. Valid range is between 1 to 5.
delete	Deletes the BLE beacon.
enable	Enables the BLE beacon.
disable	Disables the BLE beacon.
add	Adds a BLE beacon.
txpwr *value*	Configures the BLE attenuation level. You can choose to configure this for all APs, an AP group, or a specific AP. Valid range is between –52 dBm to 0.
uuid *value*	Configures universally unique identifier (UUID) for the beacon. You can choose to configure this for all APs, an AP group, or a specific AP. Enter a value in the xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx format.
ap-group *group-name*	Configures BLE beacon parameters for the AP group specified.
ap-name *ap-name*	Configures BLE beacon parameters for the AP specified.
major *mjr-value*	Configures major value for the BLE beacon. You can choose to configure this for an AP group or a specific AP.
minor *mnr-value*	Configures minor value for the BLE beacon. You can choose to configure this for an AP group or a specific AP.

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable the BLE beacon with ID value as 3:

```
(Cisco Controller) >config advanced hyperlocation ble-beacon beacon-id 3 enable
```

config advanced hotspot

To configure advanced hotspot configurations, use the **config advanced hotspot** command.

config advanced hotspot {**anqp-4way** {**disable** | **enable** | **threshold** *value* } | **cmbk-delay** *value* | **garp** {**disable** | **enable** } | **gas-limit** {**disable** | **enable** } }

Syntax Description

anqp-4way	Enables, disables, or, configures the Access Network Query Protocol (ANQP) four way fragment threshold.
disable	Disables the ANQP four way message.
enable	Enables the ANQP four way message.
threshold	Configures the ANQP fourway fragment threshold.
value	ANQP four way fragment threshold value in bytes. The range is from 10 to 1500. The default value is 1500.
cmbk-delay	Configures the ANQP comeback delay in Time Units (TUs).
value	ANQP comeback delay in Time Units (TUs). 1 TU is defined by 802.11 as 1024 usec. The range is from 1 milliseconds to 30 seconds.
garp	Disables or enables the Gratuitous ARP (GARP) forwarding to wireless network.
disable	Disables the Gratuitous ARP (GARP) forwarding to wireless network.
enable	Enables the Gratuitous ARP (GARP) forwarding to wireless network.
gas-limit	Limits the number of Generic Advertisement Service (GAS) request action frames sent to the switch by an access point in a given interval.
disable	Disables the GAS request action frame limit on access points.
enable	Enables the GAS request action frame limit on access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the ANQP four way fragment threshold value:

```
(Cisco Controller) >config advanced hotspot anqp-4way threshold 200
```

config advanced timers auth-timeout

To configure the authentication timeout, use the **config advanced timers auth-timeout** command.

config advanced timers auth-timeout *seconds*

Syntax Description

seconds	Authentication response timeout value in seconds between 10 and 600.

Command Default

The default authentication timeout value is 10 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced timers eap-timeout

To configure the Extensible Authentication Protocol (EAP) expiration timeout, use the **config advanced timers eap-timeout** command.

config advanced timers eap-timeout *seconds*

Syntax Description

seconds	EAP timeout value in seconds between 8 and 120.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the EAP expiration timeout to 10 seconds:

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

To configure the advanced Extensible Authentication Protocol (EAP) identity request delay in seconds, use the **config advanced timers eap-identity-request-delay** command.

config advanced timers eap-identity-request-delay *seconds*

Syntax Description

seconds	Advanced EAP identity request delay in number of seconds between 0 and 10.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the advanced EAP identity request delay to 8 seconds:

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config advanced timers

To configure an advanced system timer, use the **config advanced timers** command.

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* }

Syntax Description

ap-coverage-report	Configures RRM coverage report interval for all APs.
seconds	Configures the ap coverage report interval in seconds. The range is between 60 and 90 seconds. Default is 90 seconds.
ap-discovery-timeout	Configures the Cisco lightweight access point discovery timeout value.
discovery-timeout	Cisco lightweight access point discovery timeout value, in seconds. The range is from 1 to 10.
ap-fast-heartbeat	Configures the fast heartbeat timer, which reduces the amount of time it takes to detect a controller failure in access points.
local	Configures the fast heartbeat interval for access points in local mode.
flexconnect	Configures the fast heartbeat interval for access points in FlexConnect mode.
all	Configures the fast heartbeat interval for all the access points.
enable	Enables the fast heartbeat interval.
disable	Disables the fast heartbeat interval.
fast_heartbeat_seconds	Small heartbeat interval, which reduces the amount of time it takes to detect a controller failure, in seconds. The range is from 1 to 10.
ap-heartbeat-timeout	Configures Cisco lightweight access point heartbeat timeout value.
heartbeat_seconds	Cisco the Cisco lightweight access point heartbeat timeout value, in seconds. The range is from 1 to 30. This value should be at least three times larger than the fast heartbeat timer.
ap-primary-discovery-timeout	Configures the access point primary discovery request timer.
primary_discovery_timeout	Access point primary discovery request time, in seconds. The range is from 30 to 3600.
ap-primed-join-timeout	Configures the access point primed discovery timeout value.
primed_join_timeout	Access point primed discovery timeout value, in seconds. The range is from 120 to 43200.

auth-timeout	Configures the authentication timeout.
auth_timeout	Authentication response timeout value, in seconds. The range is from 10 to 600.
pkt-fwd-watchdog	Configures the packet forwarding watchdog timer to protect from fastpath deadlock.
watchdog_timer	Packet forwarding watchdog timer, in seconds. The range is from 60 to 300.
default	Configures the watchdog timer to the default value of 240 seconds.
eap-identity-request-delay	Configures the advanced Extensible Authentication Protocol (EAP) identity request delay, in seconds.
eap_identity_request_delay	Advanced EAP identity request delay, in seconds. The range is from 0 to 10.
eap-timeout	Configures the EAP expiration timeout.
eap_timeout	EAP timeout value, in seconds. The range is from 8 to 120.

Command Default

- The default access point discovery timeout is 10 seconds.
- The default access point heartbeat timeout is 30 seconds.
- The default access point primary discovery request timer is 120 seconds.
- The default authentication timeout is 10 seconds.
- The default packet forwarding watchdog timer is 240 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced.

Usage Guidelines

The Cisco lightweight access point discovery timeout indicates how often a controller attempts to discover unconnected Cisco lightweight access points.

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keepalive signal to the Cisco Wireless Controller.

The following example shows how to configure an access point discovery timeout with a timeout value of 20:

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

The following example shows how to enable the fast heartbeat interval for an access point in FlexConnect mode:

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced fastpath fastcache

To configure the fastpath fast cache control, use the **config advanced fastpath fastcache** command.

config advanced fastpath fastcache {**enable** | **disable**}

Syntax Description

enable	Enables the fastpath fast cache control.
disable	Disables the fastpath fast cache control.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the fastpath fast cache control:

```
(Cisco Controller) > config advanced fastpath fastcache enable
```

Related Commands

config advanced fastpath pkt-capture

config advanced fastpath pkt-capture

To configure the fastpath packet capture, use the **config advanced fastpath pkt-capture** command.

config advanced fastpath pkt-capture {**enable** | **disable**}

Syntax Description

enable	Enables the fastpath packet capture.
disable	Disables the fastpath packet capture.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the fastpath packet capture:

```
(Cisco Controller) > config advanced fastpath pkt-capture enable
```

Related Commands

config advanced fastpath fastcache

config advanced sip-preferred-call-no

To configure voice prioritization, use the **config advanced sip-preferred-call-no** command.

config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

Syntax Description

call_index	Call index with valid values between 1 and 6.
call_number	Preferred call number that can contain up to 27 characters.
none	Deletes the preferred call set for the specified index.

Command Default

None

Usage Guidelines

Before you configure voice prioritization, you must complete the following prerequisites:

- Set the voice to the platinum QoS level by entering the **config wlan qos** *wlan-id* **platinum** command.
- Enable the admission control (ACM) to this radio by entering the **config 802.11** {**a** | **b**} **cac** {**voice** | **video**} **acm enable** command.
- Enable the call-snooping feature for a particular WLAN by entering the **config wlan call-snoop enable** *wlan-id* command.

  To view statistics about preferred calls, enter the **show ap stats** {**802.11**{**a** | **b**} | **wlan**} *cisco_ap* command.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a new preferred call for index 2:

```
(Cisco Controller) > config advanced sip-preferred-call-no 2 0123456789
```

Related Commands

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

To configure call snooping ports, use the **config advanced sip-snooping-ports** command.

config advanced sip-snooping-ports *start_port end_port*

Syntax Description

start_port	Starting port for call snooping. The range is from 0 to 65535.
end_port	Ending port for call snooping. The range is from 0 to 65535.

Usage Guidelines

If you need only a single port for call snooping, configure the start and end port with the same number.

The port used by the CIUS tablet is 5060 and the port range used by Facetime is from 16384 to16402.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the call snooping ports:

```
(Cisco Controller) > config advanced sip-snooping-ports 4000 4500
```

Related Commands

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

To configure a primary backup controller, use the **config advanced backup-controller primary** command.

config advanced backup-controller primary *system name IP addr*

Syntax Description

system name	Configures primary|secondary backup controller.
IP addr	IP address of the backup controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

To delete a primary backup controller entry (IPv6 or IPv4), enter 0.0.0.0 for the controller IP address.

The following example shows how to configure the IPv4 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

The following example shows how to configure the IPv6 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary systemname 2001:9:6:40::623
```

The following example shows how to remove the IPv4 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

The following example shows how to remove the IPv6 primary backup controller:

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 0.0.0.0
```

Related Commands

show advanced back-up controller

config advanced backup-controller secondary

To configure a secondary backup controller, use the **config advanced backup-controller secondary** command.

config advanced backup-controller secondary *system name IP addr*

Syntax Description

system name	Configures primary|secondary backup controller.
IP addr	IP address of the backup controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

To delete a secondary backup controller entry (IPv4 or IPv6), enter 0.0.0.0 for the controller IP address.

The following example shows how to configure an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 10.10.10.10
```

The following example shows how to configure an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 2001:9:6:40::623
```

The following example shows how to remove an IPv4 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

The following example shows how to remove an IPv6 secondary backup controller:

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

Related Commands

show advanced back-up controller

config advanced client-handoff

To set the client handoff to occur after a selected number of 802.11 data packet excessive retries, use the **config advanced client-handoff** command.

config advanced client-handoff *num_of_retries*

Syntax Description

num_of_retries	Number of excessive retries before client handoff (from 0 to 255).

Command Default

The default value for the number of 802.11 data packet excessive retries is 0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command is supported only for the 1000/1510 series access points.

This example shows how to set the client handoff to 100 excessive retries:

```
(Cisco Controller) >config advanced client-handoff 100
```

config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

config advanced dot11-padding {**enable** | **disable**}

Syntax Description

enable	Enables the over-the-air frame padding.
disable	Disables the over-the-air frame padding.

Command Default

The default over-the-air frame padding is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable over-the-air frame padding:

```
(Cisco Controller) > config advanced dot11-padding enable
```

Related Commands

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

To configure the rate at which access point radios send association and authentication requests to the controller, use the **config advanced assoc-limit** command.

config advanced assoc-limit {**enable** [*number of associations per interval* | *interval*] | **disable**}

Syntax Description

enable	Enables the configuration of the association requests per access point.
disable	Disables the configuration of the association requests per access point.
number of associations per interval	(Optional) Number of association request per access point slot in a given interval. The range is from 1 to 100.
interval	(Optional) Association request limit interval. The range is from 100 to 10000 milliseconds.

Command Default

The default state of the command is disabled state.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When 200 or more wireless clients try to associate to a controller at the same time, the clients no longer become stuck in the DHCP_REQD state when you use the **config advanced assoc-limit** command to limit association requests from access points.

The following example shows how to configure the number of association requests per access point slot in a given interval of 20 with the association request limit interval of 250:

```
(Cisco Controller) >config advanced assoc-limit enable 20 250
```

config advanced max-1x-sessions

To configure the maximum number of simultaneous 802.1X sessions allowed per access point, use the **config advanced max-1x-sessions** command.

config advanced max-1x-sessions *no_of_sessions*

Syntax Description

no_of_sessions	Number of maximum 802.1x session initiation per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the maximum number of simultaneous 802.1X sessions:

```
(Cisco Controller) >config advanced max-1x-sessions 200
```

config advanced rate

To configure switch control path rate limiting, use the **config advanced rate** command.

config advanced rate {**enable** | **disable**}

Syntax Description

enable	Enables the switch control path rate limiting feature.
disable	Disables the switch control path rate limiting feature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable switch control path rate limiting:

```
(Cisco Controller) >config advanced rate enable
```

config advanced probe filter

To configure the filtering of probe requests forwarded from an access point to the controller, use the **config advanced probe filter** command.

config advanced probe filter {**enable** | **disable**}

Syntax Description

enable	Enables the filtering of probe requests.
disable	Disables the filtering of probe requests.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the filtering of probe requests forwarded from an access point to the controller:

```
(Cisco Controller) >config advanced probe filter enable
```

config advanced probe limit

To limit the number of probes sent to the WLAN controller per access point per client in a given interval, use the **config advanced probe limit** command.

config advanced probe limit *num_probes interval*

Syntax Description

num_probes	Number of probe requests (from 1 to 100) forwarded to the controller per client per access point radio in a given interval.
interval	Probe limit interval (from 100 to 10000 milliseconds).

Command Default

The default number of probe requests is 2. The default interval is 500 milliseconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to set the number of probes per access point per client to 5 and the probe interval to 800 milliseconds:

```
(Cisco Controller) >config advanced probe limit 5 800
```

config advanced timers

To configure an advanced system timer, use the **config advanced timers** command.

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* }

Syntax Description

ap-coverage-report	Configures RRM coverage report interval for all APs.
seconds	Configures the ap coverage report interval in seconds. The range is between 60 and 90 seconds. Default is 90 seconds.
ap-discovery-timeout	Configures the Cisco lightweight access point discovery timeout value.
discovery-timeout	Cisco lightweight access point discovery timeout value, in seconds. The range is from 1 to 10.
ap-fast-heartbeat	Configures the fast heartbeat timer, which reduces the amount of time it takes to detect a controller failure in access points.
local	Configures the fast heartbeat interval for access points in local mode.
flexconnect	Configures the fast heartbeat interval for access points in FlexConnect mode.
all	Configures the fast heartbeat interval for all the access points.
enable	Enables the fast heartbeat interval.
disable	Disables the fast heartbeat interval.
fast_heartbeat_seconds	Small heartbeat interval, which reduces the amount of time it takes to detect a controller failure, in seconds. The range is from 1 to 10.
ap-heartbeat-timeout	Configures Cisco lightweight access point heartbeat timeout value.
heartbeat_seconds	Cisco the Cisco lightweight access point heartbeat timeout value, in seconds. The range is from 1 to 30. This value should be at least three times larger than the fast heartbeat timer.
ap-primary-discovery-timeout	Configures the access point primary discovery request timer.
primary_discovery_timeout	Access point primary discovery request time, in seconds. The range is from 30 to 3600.
ap-primed-join-timeout	Configures the access point primed discovery timeout value.
primed_join_timeout	Access point primed discovery timeout value, in seconds. The range is from 120 to 43200.

auth-timeout	Configures the authentication timeout.
auth_timeout	Authentication response timeout value, in seconds. The range is from 10 to 600.
pkt-fwd-watchdog	Configures the packet forwarding watchdog timer to protect from fastpath deadlock.
watchdog_timer	Packet forwarding watchdog timer, in seconds. The range is from 60 to 300.
default	Configures the watchdog timer to the default value of 240 seconds.
eap-identity-request-delay	Configures the advanced Extensible Authentication Protocol (EAP) identity request delay, in seconds.
eap_identity_request_delay	Advanced EAP identity request delay, in seconds. The range is from 0 to 10.
eap-timeout	Configures the EAP expiration timeout.
eap_timeout	EAP timeout value, in seconds. The range is from 8 to 120.

Command Default

- The default access point discovery timeout is 10 seconds.
- The default access point heartbeat timeout is 30 seconds.
- The default access point primary discovery request timer is 120 seconds.
- The default authentication timeout is 10 seconds.
- The default packet forwarding watchdog timer is 240 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced.

Usage Guidelines

The Cisco lightweight access point discovery timeout indicates how often a controller attempts to discover unconnected Cisco lightweight access points.

The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keepalive signal to the Cisco Wireless Controller.

The following example shows how to configure an access point discovery timeout with a timeout value of 20:

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

The following example shows how to enable the fast heartbeat interval for an access point in FlexConnect mode:

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

The following example shows how to configure the authentication timeout to 20 seconds:

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config ap 802.1Xuser

To configure the global authentication username and password for all access points currently associated with the controller as well as any access points that associate with the controller in the future, use the **config ap 802.1Xuser** command.

config ap 802.1Xuser add username *ap-username* **password** *ap-password* {**all** | *cisco_ap*}

Syntax Description

add username	Specifies to add a username.
ap-username	Username on the Cisco AP.
password	Specifies to add a password.
ap-password	Password.
cisco_ap	Specific access point.
all	Specifies all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must enter a strong *password*. Strong passwords have the following characteristics:

- They are at least eight characters long.
- They contain a combination of uppercase and lowercase letters, numbers, and symbols.
- They are not a word in any language.

You can set the values for a specific access point.

This example shows how to configure the global authentication username and password for all access points:

```
(Cisco Controller) >config ap 802.1Xuser add username cisco123 password cisco2020 all
```

config ap 802.1Xuser delete

To force a specific access point to use the controller's global authentication settings, use the **config ap 802.1Xuser delete** command.

config ap 802.1Xuser delete *cisco_ap*

Syntax Description

cisco_ap	Access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete access point AP01 to use the controller's global authentication settings:

```
(Cisco Controller) >config ap 802.1Xuser delete AP01
```

config ap 802.1Xuser disable

To disable authentication for all access points or for a specific access point, use the **config ap 802.1Xuser disable** command.

config ap 802.1Xuser disable {**all** | *cisco_ap*}

Syntax Description

disable	Disables authentication.
all	Specifies all access points.
cisco_ap	Access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can disable 802.1X authentication for a specific access point only if global 802.1X authentication is not enabled. If global 802.1X authentication is enabled, you can disable 802.1X for all access points only.

The following example shows how to disable the authentication for access point cisco_ap1:

```
(Cisco Controller) >config ap 802.1Xuser disable
```

config advanced dot11-padding

To enable or disable over-the-air frame padding, use the **config advanced dot11-padding** command.

config advanced dot11-padding {**enable** | **disable**}

Syntax Description

enable	Enables the over-the-air frame padding.
disable	Disables the over-the-air frame padding.

Command Default

The default over-the-air frame padding is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable over-the-air frame padding:

```
(Cisco Controller) > config advanced dot11-padding enable
```

Related Commands

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

To configure a Cisco lightweight access point or to add or delete a third-party (foreign) access point, use the **config ap** command.

config ap {{**enable** | **disable**} *cisco_ap* | {**add** | **delete**} *MAC port* {**enable** | **disable**} *IP_address*}

Syntax Description

enable	Enables the Cisco lightweight access point.
disable	Disables the Cisco lightweight access point.
cisco_ap	Name of the Cisco lightweight access point.
add	Adds foreign access points.
delete	Deletes foreign access points.
MAC	MAC address of a foreign access point.
port	Port number through which the foreign access point can be reached.
IP_address	IP address of the foreign access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6.

The following example shows how to disable lightweight access point AP1:

```
(Cisco Controller) >config ap disable AP1
```

The following example shows how to add a foreign access point with MAC address 12:12:12:12:12:12 and IP address 192.12.12.1 from port 2033:

```
(Cisco Controller) >config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```

config ap aid-audit

To configure the Cisco lightweight access point AID audit mechanism, use the **config ap aid-audit** command.

config ap aid-audit {**enable** | **disable**}

Syntax Description

aid-audit	Configures AID audit mechanism.
enable	Enables AID audit mechanism.
disable	Disables AID audit mechanism.

Command Default

Disabled.

Command History

Release	Modification
8.6	This command was introduced.

The following example shows how to enable AP aid-audit:

```
(Cisco Controller) >config ap aid-audit enable
```

config ap antenna band-mode

To configure a Cisco AP antenna's band mode as either single or dual, use the **config ap antenna band-mode** command.

config ap antenna band-mode {**single** | **dual**} *cisco-ap*

Syntax Description

single	Configures single band antenna mode for a Cisco AP.
dual	Configures dual band antenna mode for a Cisco AP.
cisco-ap	Cisco AP name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.
8.3 and later releases	The **antenna-band-mode** parameter was modified to **antenna band-mode**.

config ap atf 802.11

Configure Cisco Airtime Fairness at an AP level by using the **config ap atf 802.11** command.

config ap atf 802.11 {**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-name*} | {**optimization** {**enable** | **disable**}}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b/g network settings
mode	Configures the granularity of Cisco ATF enforcement
disable	Disables Cisco ATF
monitor	Configures Cisco ATF in monitor mode
enforce-policy	Configures Cisco ATF in enforcement mode
ap-name	AP name that you must specify
optimization	Configures airtime optimization
enable	Enables airtime optimization
disable	Disables airtime optimization

Command History

Release	Modification
8.1	This command was introduced

To enable airtime optimization on an 802.11a network for a Cisco AP, *my-ap*, enter the following command:

```
(Cisco Controller) >config ap atf 802.11a optimization enable my-ap
```

config ap atf 802.11 client-access airtime-allocation

To configure override of ATF airtime allocation on mesh AP, use the **config ap atf 802.11 client-access airtime-allocation override** {**enable** | **disable**} command.

config ap atf 802.11{**a** | **b**} **client-access airtime-allocation** *%-of-airtime-allocation-bw-5-to-90 mesh-ap-name* **override** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b/g network settings
%-of-airtime-allocation-bw-5-to-90	Percentage of airtime allocation for client access. Valid range is between 5 and 90. This percentage of airtime allocation impacts both the client and the uplink backhaul percentage.
mesh-ap-name	Name of the mesh AP
override	Allows override of ATF airtime allocation on the mesh AP
enable	Enables airtime allocation override
disable	Disables airtime allocation override

Command History

Release	Modification
8.4	This command was introduced

On an 802.11a network, to configure override of ATF airtime allocation on a mesh AP, *map1*, enter the following command:

```
(Cisco Controller) >config ap atf 802.11a client-access airtime-allocation
10 override map1 enable
```

config ap atf 802.11 policy

To configure AP-level override for Cisco ATF policy on a WLAN, enter this command:

confit ap atf 802.11 {**a** | **b**} **policy** *wlan-id policy-name ap-name* **override** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b network settings
policy	Specifies the Cisco ATF policy
wlan-id	WLAN ID or Remote LAN ID that you must specify
policy-name	Cisco ATF policy name that you must specify
ap-name	Name of the AP that you must specify
override	Configures ATF policy override for a WLAN in the AP group
enable	Enables ATF policy override for a WLAN in the AP group
disable	Disables ATF policy override for a WLAN in the AP group

Command History

Release	Modification
8.1	This command was introduced

config ap autoconvert

To automatically convert all access points to FlexConnect mode or Monitor mode upon associating with the controller, use the **config ap autoconvert** command.

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

Syntax Description

flexconnect	Configures all the access points automatically to FlexConnect mode.
monitor	Configures all the access points automatically to monitor mode.
disable	Disables the autoconvert option on the access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When access points in local mode connect to a Cisco 7500 Series Wireless Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Wireless Controller, the access points must be in FlexConnect mode or Monitor mode.

The command can also be used for conversion of AP modes in Cisco 5520, 8540, and 8510 Series Wireless Controller platforms.

The following example shows how to automatically convert all access points to the FlexConnect mode:

```
(Cisco Controller) >config ap autoconvert flexconnect
```

The following example shows how to disable the autoconvert option on the APs:

```
(Cisco Controller) >config ap autoconvert disable
```

config ap bhrate

To configure the Cisco bridge backhaul Tx rate, use the **config ap bhrate** command.

config ap bhrate {*rate* | **auto**} *cisco_ap*

Syntax Description

rate	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.
auto	Configures the auto data rate.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

The default status of the command is set to Auto.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When the bridge data rate is set to **auto**, the mesh backhaul chooses the highest rate where the next higher rate cannot be used due to unsuitable conditions for that specific rate (and not because of conditions that affect all rates).

The following example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
(Cisco Controller) >config ap bhrate 54000 AP01
```

config ap bridgegroupname

To set or delete a bridge group name on a Cisco lightweight access point, use the **config ap bridgegroupname** command.

config ap bridgegroupname {**set** *groupname* | **delete** | {**strict-matching** {**enable** | **disable**} } }*cisco_ap*

Syntax Description

set	Sets a Cisco lightweight access point's bridge group name.
groupname	Bridge group name.
delete	Deletes a Cisco lightweight access point's bridge group name.
cisco_ap	Name of a Cisco lightweight access point.
strict-matching	Restricts the possible parent list, if the MAP has a non-default BGN, and the potential parent has a different BGN
enable	Enables a Cisco lightweight access point's group name.
disable	Disables a Cisco lightweight access point's group name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The **strict-matching** parameter was added.

Usage Guidelines

Only access points with the same bridge group name can connect to each other. Changing the AP bridgegroupname may strand the bridge AP.

The following example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
(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

To configure Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **config ap bridging** command.

config ap bridging {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the Ethernet-to-Ethernet bridging on a Cisco lightweight access point.
disable	Disables Ethernet-to-Ethernet bridging.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable bridging on an access point:

```
(Cisco Controller) >config ap bridging enable nyc04-44-1240
```

The following example shows hot to disable bridging on an access point:

```
(Cisco Controller) >config ap bridging disable nyc04-44-1240
```

config ap cdp

To configure the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **config ap cdp** command.

config ap cdp {**enable** | **disable** | **interface** {**ethernet** *interface_number* | **slot** *slot_id*}} {*cisco_ap* | **all**}

Syntax Description

enable	Enables CDP on an access point.
disable	Disables CDP on an access point.
interface	Configures CDP in a specific interface.
ethernet	Configures CDP for an ethernet interface.
interface_number	Ethernet interface number between 0 and 3.
slot	Configures CDP for a radio interface.
slot_id	Slot number between 0 and 3.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

Enabled on radio interfaces of mesh APs and disabled on radio interfaces of non-mesh APs. Enabled on Ethernet interfaces of all APs.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The **config ap cdp disable all** command disables CDP on all access points that are joined to the controller and all access points that join in the future. CDP remains disabled on both current and future access points even after the controller or access point reboots. To enable CDP, enter the **config ap cdp enable all** command.

Note CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points joined to the controller, you may disable and then reenable CDP on individual access points using the **config ap cdp** {**enable** | **disable**} *cisco_ap command*. After you disable CDP on all access points joined to the controller, you may not enable and then disable CDP on individual access points.

The following example shows how to enable CDP on all access points:

```
(Cisco Controller) >config ap cdp enable all
```

The following example shows how to disable CDP on ap02 access point:

```
(Cisco Controller) >config ap cdp disable ap02
```

The following example shows how to enable CDP for Ethernet interface number 2 on all access points:

```
(Cisco Controller) >config ap cdp ethernet 2 enable all
```

config ap cert-expiry-ignore

To configure the device certificate date validation check, use the **config ap cert-expiry-ignore** command.

config ap cert-expiry-ignore {**mic** | **ssc** {**enable** | **disable** }

Syntax Description

cert-expiry-ignore	Configures certifictate expiry-ignore check operation.
mic	Configures cert-expiry-ignore check operation for MIC.
ssc	Configures cert-expiry-ignore check operation for SSC.
enable	Enabling will ignore the lifetime-check.
disable	Disabling will do the lifetime-check.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.7	This command was enhanced to include certificate date validation check for the controller.

The following example shows how to ignore lifetime check on MIC certificate:

```
(Cisco Controller) >config ap cert-expiry-ignore mic enable
```

config ap core-dump

To configure a Cisco lightweight access point's memory core dump, use the **config ap core-dump** command.

config ap core-dump {**disable** | **enable** *tftp_server_ipaddress filename* {**compress** | **uncompress**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the Cisco lightweight access point's memory core dump setting.
disable	Disables the Cisco lightweight access point's memory core dump setting.
tftp_server_ipaddress	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point uses to label the core file.
compress	Compresses the core dump file.
uncompress	Uncompresses the core dump file.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Note If an AP itself is configured with the name 'all', then the 'all access points' case takes precedence over the AP that is named 'all'.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6.

Usage Guidelines

The access point must be able to reach the TFTP server. This command is applicable for both IPv4 and IPv6 addresses.

The following example shows how to configure and compress the core dump file:

```
(Cisco Controller) >config ap core-dump enable 209.165.200.225 log compress AP02
```

config ap crash-file clear-all

To delete all crash and radio core dump files, use the **config ap crash-file clear-all** command.

config ap crash-file clear-all

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete all crash files:

```
(Cisco Controller) >config ap crash-file clear-all
```

config ap crash-file delete

To delete a single crash or radio core dump file, use the **config ap crash-file delete** command.

config ap crash-file delete *filename*

Syntax Description

filename	Name of the file to delete.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete crash file 1:

```
(Cisco Controller) >config ap crash-file delete crash_file_1
```

config ap crash-file get-crash-file

To collect the latest crash data for a Cisco lightweight access point, use the **config ap crash-file get-crash-file** command.

config ap crash-file get-crash-file *cisco_ap*

Syntax Description

cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **transfer upload datatype** command to transfer the collected data to the Cisco wireless LAN controller.

The following example shows how to collect the latest crash data for access point AP3:

```
(Cisco Controller) >config ap crash-file get-crash-file AP3
```

config ap crash-file get-radio-core-dump

To get a Cisco lightweight access point's radio core dump, use the **config ap crash-file get-radio-core-dump** command.

config ap crash-file get-radio-core-dump *slot_id cisco_ap*

Syntax Description

slot_id	Slot ID (either 0 or 1).
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to collect the radio core dump for access point AP02 and slot 0:

```
(Cisco Controller) >config ap crash-file get-radio-core-dump 0 AP02
```

config ap dhcp release-override

To configure DHCP release override on Cisco APs, use the **config ap dhcp release-override** command.

config ap dhcp release-override {**enable** | **disable**} {*cisco-ap-name* | **all**}

Syntax Description

enable	Enables DHCP release override and sets number of DHCP releases sent by AP to 1. To be used as a workaround for a few DHCP servers that mark the AP's IP address as bad. We recommend that you use this configuration only in highly reliable networks.
disable	Disables DHCP release override and sets number of DHCP releases sent by AP to 3, which is the default value. This ensures that the DHCP server receives the release message even if one of the packets is lost.
cisco-ap-name	Configuration is applied to the Cisco AP that you enter
all	Configuration is applied to all Cisco APs

Command Default

Disabled

Command History

Release	Modification
8.2	This command was introduced.

Usage Guidelines

Use this command when you are using Cisco lightweight APs with Windows Server 2008 R2 or 2012 as the DHCP server.

config ap dtls-cipher-suite

To enable new cipher suites for DTLS connection between AP and controller, use the **config ap dtls-cipher-suite** command.

config ap dtls-cipher-suite { **RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA** }

Syntax Description

RSA-AES256-SHA256	Cipher suite using either RSA key exchange or authentication, using 256 bit AES and SHA 256.
RSA-AES256-SHA	Cipher suite using either RSA key exchange or authentication, using 256 bit AES and SHA.
RSA-AES128-SHA	Cipher suite using either RSA key exchange or authentication, using 128 bit AES and SHA.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable RSA cipher suites using 256 bit AES and SHA 256 for DTLS connection between AP and controller:

```
(Cisco Controller) >config ap dtls-cipher-suite RSA-AES256-SHA256
```

config ap dtls-version

To configure the cipher DTLS version, use the **config ap dtls-version** command.

config ap dtls-version { **dtls1.0 | dtls1.2 | dtls_all** }

Syntax Description

dtls1.0	Select DTLS 1.0 version
dtls1.2	Select DTLS 1.2 version
dtls_all	Select all DTLS versions for backward compatibility

Command Default

None

Command History

Release	Modification
8.3.111.0	This command was introduced.

The following example shows how to configure cipher dtls version 1.2:

```
(Cisco Controller) > config ap dtls-version dtls1.2
```

config ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **config ap ethernet duplex** command.

config ap ethernet duplex [**auto** | **half** | **full**] **speed** [**auto** | **10** | **100** | **1000**] { **all** | *cisco_ap*}

Syntax Description

auto	(Optional) Specifies the Ethernet port duplex auto settings.
half	(Optional) Specifies the Ethernet port duplex half settings.
full	(Optional) Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
auto	(Optional) Specifies the Ethernet port speed to auto.
10	(Optional) Specifies the Ethernet port speed to 10 Mbps.
100	(Optional) Specifies the Ethernet port speed to 100 Mbps.
1000	(Optional) Specifies the Ethernet port speed to 1000 Mbps.
all	Specifies the Ethernet port setting for all connected access points.
cisco_ap	Cisco access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Ethernet port duplex half settings as 10 Mbps for all access points:

```
(Cisco Controller) >config ap ethernet duplex half speed 10 all
```

config ap ethernet tag

To configure VLAN tagging of the Control and Provisioning of Wireless Access Points protocol (CAPWAP) packets, use the **config ap ethernet tag** command.

config ap ethernet tag {**id** *vlan_id* | **disable**} {*cisco_ap* | **all**}

Syntax Description

id	Specifies the VLAN id.
vlan_id	ID of the trunk VLAN.
disable	Disables the VLAN tag feature. When you disable VLAN tagging, the access point untags the CAPWAP packets.
cisco_ap	Name of the Cisco AP.
all	Configures VLAN tagging on all the Cisco access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

After you configure VLAN tagging, the configuration comes into effect only after the access point reboots.

You cannot configure VLAN tagging on mesh access points.

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the Cisco Prime Infrastructure, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

The following example shows how to configure VLAN tagging on a trunk VLAN:

```
(Cisco Controller) >config ap ethernet tag 6 AP1
```

config ap autoconvert

To automatically convert all access points to FlexConnect mode or Monitor mode upon associating with the controller, use the **config ap autoconvert** command.

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

Syntax Description

flexconnect	Configures all the access points automatically to FlexConnect mode.
monitor	Configures all the access points automatically to monitor mode.
disable	Disables the autoconvert option on the access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When access points in local mode connect to a Cisco 7500 Series Wireless Controller, they do not serve clients. The access point details are available in the controller. To enable access points to serve clients or perform monitoring related tasks when connected to the Cisco 7500 Series Wireless Controller, the access points must be in FlexConnect mode or Monitor mode.

The command can also be used for conversion of AP modes in Cisco 5520, 8540, and 8510 Series Wireless Controller platforms.

The following example shows how to automatically convert all access points to the FlexConnect mode:

```
(Cisco Controller) >config ap autoconvert flexconnect
```

The following example shows how to disable the autoconvert option on the APs:

```
(Cisco Controller) >config ap autoconvert disable
```

config ap flexconnect central-dhcp

To enable central-DHCP on a FlexConnect access point in a WLAN, use the **config ap flexconnect central-dhcp** command.

config ap flexconnect central-dhcp *wlan_id cisco_ap* [**add** | **delete**] {**enable** | **disable**} **override dns** {**enable** | **disable**} **nat-pat** {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
cisco_ap	Name of the Cisco lightweight access point.
add	(Optional) Adds a new WLAN DHCP mapping.
delete	(Optional) Deletes a WLAN DHCP mapping.
enable	Enables central-DHCP on a FlexConnect access point. When you enable this feature, the DHCP packets received from the access point are centrally switched to the controller and then forwarded to the corresponding VLAN based on the AP and the SSID.
disable	Disables central-DHCP on a FlexConnect access point.
override dns	Overrides the DNS server address on the interface assigned by the controller. When you override DNS in centrally switched WLANs, the clients get their DNS server IP address from the AP and not from the controller.
enable	Enables the Override DNS feature on a FlexConnect access point.
disable	Disables the Override DNS feature on a FlexConnect access point.
nat-pat	Network Address Translation (NAT) and Port Address Translation (PAT) that you can enable or disable.
enable	Enables NAT-PAT on a FlexConnect access point.
disable	Deletes NAT-PAT on a FlexConnect access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable central-DHCP, Override DNS, and NAT-PAT on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect central-dhcp 1 ap1250 enable override dns enable
 nat-pat enable
```

config ap flexconnect local-split

To configure a local-split tunnel on a FlexConnect access point, use the **config ap flexconnect local-split** command.

config ap flexconnect local-split *wlan_id cisco_ap* {**enable** | **disable**} **acl** *acl_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
cisco_ap	Name of the FlexConnect access point.
enable	Enables local-split tunnel on a FlexConnect access point.
disable	Disables local-split tunnel feature on a FlexConnect access point.
acl	Configures a FlexConnect local-split access control list.
acl_name	Name of the FlexConnect access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command allows you to configure a local-split tunnel in a centrally switched WLAN using a FlexConnect ACL. A local split tunnel supports only for unicast Layer 4 IP traffic as NAT/PAT does not support multicast IP traffic.

The following example shows how to configure a local-split tunnel using a FlexConnect ACL:

```
(Cisco Controller) >config ap flexconnect local-split 6 AP2 enable acl flex6
```

config ap flexconnect module-vlan

To configure VLAN tagging for Cisco USC 8x18 Dual Mode Module in FlexConnect Local Switching, use the **config ap flexconnect module-vlan** command.

config ap flexconnect module-vlan { { **enable** *ap-name* [**vlan** *vlan-id*] } | { { **disable** | **remove** } *ap-name* } }

Syntax Description

enable *ap-name*	Enables FlexConnect local switching for the external module of the specified Cisco AP with native VLAN
enable *ap-name* **vlan** *vlan-id*	Enables FlexConnect local switching with non-native VLAN for the external module of the specified Cisco AP
disable *ap-name*	Disables FlexConnect local switching for the external module of the specified Cisco AP
remove *ap-name*	Removes the AP-specific external module VLAN configuration

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to enable FlexConnect local switching with non-native VLAN for the external module of a Cisco AP:

```
(Cisco Controller) >config ap flexconnect module-vlan enable 3600i-ap vlan4
```

config ap flexconnect policy

To configure a policy ACL on a FlexConnect access point, use the **config ap flexconnect policy** command.

config ap flexconnect policy {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a policy ACL on a FlexConnect access point.
deletes	Deletes a policy ACL on a FlexConnect access point.
acl_name	Name of the ACL.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to add a policy ACL on a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

config ap flexconnect radius auth set

To configure a primary or secondary RADIUS server for a specific FlexConnect access point, use the **config ap flexconnect radius auth set** command.

config ap flexconnect radius auth set {**primary** | **secondary**} *ip_address auth_port secret*

Syntax Description

primary	Specifies the primary RADIUS server for a specific FlexConnect access point
secondary	Specifies the secondary RADIUS server for a specific FlexConnect AP
ip_address	IP address of the RADIUS server
auth_port secret	Name of the port
secret	RADIUS server secret

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a primary RADIUS server for a specific access point:

```
(Cisco Controller) >config ap flexconnect radius auth set primary 192.12.12.1
```

config ap flexconnect vlan

To enable or disable VLAN tagging for a FlexConnect access, use the **config ap flexconnect vlan** command.

config ap flexconnect vlan { **enable** | **disable** } *cisco_ap*

Syntax Description

enable	Enables the access point's VLAN tagging.
disable	Disables the access point's VLAN tagging.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Disabled. Once enabled, WLANs enabled for local switching inherit the VLAN assigned at the controller.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable the access point's VLAN tagging for a FlexConnect access:

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

config ap flexconnect vlan add

To add a VLAN to a FlexConnect access point, use the **config ap flexconnect vlan add** command.

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
acl	ACL name that contains up to 32 alphanumeric characters.
in-acl	Inbound ACL name that contains up to 32 alphanumeric characters.
out-acl	Outbound ACL name that contains up to 32 alphanumeric characters.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

config ap flexconnect vlan native

To configure a native VLAN for a FlexConnect access point, use the **config ap flexconnect vlan native** command.

config ap flexconnect vlan native *vlan-id cisco_ap*

Syntax Description

vlan-id	VLAN identifier.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a native VLAN for a FlexConnect access point mode:

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

config ap flexconnect vlan wlan

To assign a VLAN ID to a FlexConnect access point, use the **config ap flexconnect vlan wlan** command.

config ap flexconnect vlan wlan *wlan-id vlan-id cisco_ap*

Syntax Description

wlan-id	WLAN identifier
vlan-id	VLAN identifier (1 - 4094).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

VLAN ID associated to the WLAN.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to assign a VLAN ID to a FlexConnect access point:

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

config ap flexconnect web-auth

To configure a FlexConnect ACL for external web authentication in locally switched WLANs, use the **config ap flexconnect web-auth** command.

config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* { **enable** | **disable** }

Syntax Description

wlan	Specifies the wireless LAN to be configured with a FlexConnect ACL.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
cisco_ap	Name of the FlexConnect access point.
acl_name	Name of the FlexConnect ACL.
enable	Enables the FlexConnect ACL on the locally switched wireless LAN.
disable	Disables the FlexConnect ACL on the locally switched wireless LAN.

Command Default

FlexConnect ACL for external web authentication in locally switched WLANs is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The FlexConnect ACLs that are specific to an AP have the highest priority. The FlexConnect ACLs that are specific to WLANs have the lowest priority.

The following example shows how to enable FlexConnect ACL for external web authentication on WLAN 6:

```
(Cisco Controller) >config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable
```

config ap flexconnect web-policy acl

To configure a Web Policy FlexConnect ACL on an access point, use the **config ap flexconnect web-policy acl** command.

config ap flexconnect web-policy acl {**add** | **delete**} *acl_name*

Syntax Description

add	Adds a Web Policy FlexConnect ACL on an access point.
delete	Deletes Web Policy FlexConnect ACL on an access point.
acl_name	Name of the Web Policy FlexConnect ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a Web Policy FlexConnect ACL on an access point:

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```

config ap flexconnect wlan

To configure a FlexConnect access point in a locally switched WLAN, use the **config ap flexconnect wlan** command.

config ap flexconnect wlan l2acl { **add** *wlan_id cisco_ap acl_name* | **delete** *wlan_id cisco_ap* }

Syntax Description

add	Adds a Layer 2 ACL to the FlexConnect access point.
wlan_id	Wireless LAN identifier from 1 to 512.
cisco_ap	Name of the Cisco lightweight access point.
acl_name	Layer 2 ACL name. The name can be up to 32 alphanumeric characters.
delete	Deletes a Layer 2 ACL from the FlexConnect access point.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

- You can create a maximum of 16 rules for a Layer 2 ACL.
- You can create a maximum of 64 Layer 2 ACLs on a controller.
- A maximum of 16 Layer 2 ACLs are supported per AP because an AP supports a maximum of 16 WLANs.
- Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an AP does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to configure a Layer 2 ACL on a FlexConnect AP.

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_l2_1
```

config ap group-name

To specify a descriptive group name for a Cisco lightweight access point, use the **config ap group-name** command.

config ap group-name *groupname cisco_ap*

Syntax Description

groupname	Descriptive name for the access point group.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

The following example shows how to configure a descriptive name for access point AP01:

```
(Cisco Controller) >config ap group-name superusers AP01
```

config ap hotspot

To configure hotspot parameters on an access point, use the **config ap hotspot** command.

config ap hotspot venue {**type** *group_code type_code* | **name** {**add** *language_code venue_name* | **delete**}} *cisco_ap*

Syntax Description

venue	Configures venue information for given AP group.
type	Configures the type of venue for given AP group.
group_code	Venue group information for given AP group. The following options are available: • 0—UNSPECIFIED • 1—ASSEMBLY • 2—BUSINESS • 3—EDUCATIONAL • 4—FACTORY-INDUSTRIAL • 5—INSTITUTIONAL • 6—MERCANTILE • 7—RESIDENTIAL • 8—STORAGE • 9—UTILITY-MISC • 10—VEHICULAR • 11—OUTDOOR

type_code

Venue type information for the AP group.

For venue group 1 (ASSEMBLY), the following options are available:

- 0—UNSPECIFIED ASSEMBLY
- 1—ARENA
- 2—STADIUM
- 3—PASSENGER TERMINAL
- 4—AMPHITHEATER
- 5—AMUSEMENT PARK
- 6—PLACE OF WORSHIP
- 7—CONVENTION CENTER
- 8—LIBRARY
- 9—MUSEUM
- 10—RESTAURANT
- 11—THEATER
- 12—BAR
- 13—COFFEE SHOP
- 14—ZOO OR AQUARIUM
- 15—EMERGENCY COORDINATION CENTER

For venue group 2 (BUSINESS), the following options are available:

- 0—UNSPECIFIED BUSINESS
- 1—DOCTOR OR DENTIST OFFICE
- 2—BANK
- 3—FIRE STATION
- 4—POLICE STATION
- 6—POST OFFICE
- 7—PROFESSIONAL OFFICE
- 8—RESEARCH AND DEVELOPMENT FACILITY
- 9—ATTORNEY OFFICE

For venue group 3 (EDUCATIONAL), the following options are available:

- 0—UNSPECIFIED EDUCATIONAL
- 1—PRIMARY SCHOOL
- 2—SECONDARY SCHOOL

- 3—UNIVERSITY OR COLLEGE

For venue group 4 (FACTORY-INDUSTRIAL), the following options are available:

- 0—UNSPECIFIED FACTORY AND INDUSTRIAL
- 1—FACTORY

For venue group 5 (INSTITUTIONAL), the following options are available:

- 0—UNSPECIFIED INSTITUTIONAL
- 1—HOSPITAL
- 2—LONG-TERM CARE FACILITY
- 3—ALCOHOL AND DRUG RE-HABILITATION CENTER
- 4—GROUP HOME
- 5 :PRISON OR JAIL

type_code

For venue group 6 (MERCANTILE), the following options are available:

- 0—UNSPECIFIED MERCANTILE
- 1—RETAIL STORE
- 2—GROCERY MARKET
- 3—AUTOMOTIVE SERVICE STATION
- 4—SHOPPING MALL
- 5—GAS STATION

For venue group 7 (RESIDENTIAL), the following options are available:

- 0—UNSPECIFIED RESIDENTIAL
- 1—PRIVATE RESIDENCE
- 2—HOTEL OR MOTEL
- 3—DORMITORY
- 4—BOARDING HOUSE

For venue group 8 (STORAGE), the option is:

- 0—UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the option is:

- 0—UNSPECIFIED UTILITY AND MISCELLANEOUS

For venue group 10 (VEHICULAR), the following options are available:

- 0—UNSPECIFIED VEHICULAR
- 1—AUTOMOBILE OR TRUCK
- 2—AIRPLANE
- 3—BUS
- 4—FERRY
- 5—SHIP OR BOAT
- 6—TRAIN
- 7—MOTOR BIKE

For venue group 11 (OUTDOOR), the following options are available:

- 0—UNSPECIFIED OUTDOOR
- 1—MINI-MESH NETWORK
- 2—CITY PARK
- 3—REST AREA

- 4—TRAFFIC CONTROL
- 5—BUS STOP
- 6—KIOSK

name	Configures the name of venue for this access point.
language_code	ISO-639 encoded string defining the language used at the venue. This string is a three-character language code. For example, you can enter ENG for English.
venue_name	Venue name for this access point. This name is associated with the basic service set (BSS) and is used in cases where the SSID does not provide enough information about the venue. The venue name is case sensitive and can be up to 252 alphanumeric characters.
add	Adds the HotSpot venue name for this access point.
delete	Deletes the HotSpot venue name for this access point.
cisco_ap	Name of the Cisco access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the venue group as educational and venue type as university:

```
(Cisco Controller) >config ap hotspot venue type 3 3
```

config ap image predownload

To configure an image on a specified access point, use the **config ap image predownload** command.

config ap image predownload {**abort** | **primary** | **backup**} {*cisco_ap* | **all**}

Syntax Description

abort	Terminates the predownload image process.
primary	Predownloads an image to a Cisco access point from the controller's primary image.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points to predownload an image.
(Cisco Controller) >	

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to predownload an image to an access point from the primary image:

```
(Cisco Controller) >config ap image predownload primary all
```

config ap image swap

To swap an access point's primary and backup images, use the **config ap image swap** command.

config ap image swap {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points to interchange the boot images.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to swap an access point's primary and secondary images:

```
(Cisco Controller) >config ap image swap all
```

config ap ipsla

To configure the IP Service Level Agreements of the AP, use the **config ap ipsla** command.

config ap ipsla { **enable** | **disable** } *ap_name*

Syntax Description

Enable	Enables IPSLA on an AP.
Disable	Disables IPSLA on an AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable IPSLA on an AP:

```
(Cisco Controller) > config ap ipsla cz2340212
```

config ap led-state

To configure the LED state of an access point or to configure the flashing of LEDs, use the **config ap led-state** command.

config ap led-state {**enable** | **disable**} {*cisco_ap* | **all**}

config ap led-state flash {*seconds* | **indefinite** | **disable**} {*cisco_ap* | **dual-band**}

Syntax Description

enable	Enables the LED state of an access point.
disable	Disables the LED state of an access point.
cisco_ap	Name of a Cisco lightweight access point.
flash	Configure the flashing of LEDs for an access point.
seconds	Duration that the LEDs have to flash. The range is from 1 to 3600 seconds.
indefinite	Configures indefinite flashing of the access point's LED.
dual-band	Configures the LED state for all dual-band access points.

Usage Guidelines

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

LEDs on access points with dual-band radio module will flash green and blue when you execute the led state flash command.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the LED state for an access point:

```
(Cisco Controller) >config ap led-state enable AP02
```

The following example shows how to enable the flashing of LEDs for dual-band access points:

```
(Cisco Controller) >config ap led-state flash 20 dual-band
```

config ap link-encryption

To configure the Datagram Transport Layer Security (DTLS) data encryption for access points on the 5500 series controller, use the **config ap link-encryption** command.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

config ap link-encryption {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the DTLS data encryption for access points.
disable	Disables the DTLS data encryption for access points.
cisco_ap	Name of a Cisco lightweight access point.
all	Specifies all access points.

Command Default

DTLS data encryption is enabled automatically for OfficeExtend access points but disabled by default for all other access points.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Only Cisco 5500 Series Controllers support DTLS data encryption. This feature is not available on other controller platforms. If an access point with data encryption enabled tries to join any other controller, the access point joins the controller, but data packets are sent unencrypted.

Only Cisco 1130, 1140, 1240, and 1250 series access points support DTLS data encryption, and data-encrypted access points can join a Cisco 5500 Series Controller only if the wplus license is installed on the controller. If the wplus license is not installed, the access points cannot join the controller.

The following example shows how to enable the data encryption for an access point:

```
(Cisco Controller) >config ap link-encryption enable AP02
```

config ap link-latency

To configure link latency for a specific access point or for all access points currently associated to the controller, use the **config ap link-latency** command:

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

config ap link-latency {**enable** | **disable** | **reset**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables the link latency for an access point.
disable	Disables the link latency for an access point.
reset	Resets all link latency for all access points.
cisco_ap	Name of the Cisco lightweight access point.
all	Specifies all access points.

Command Default

By default, link latency is in disabled state.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the controller. It does not apply to access points that join in the future.

The following example shows how to enable the link latency for all access points:

```
(Cisco Controller) >config ap link-latency enable all
```

config ap location

To modify the descriptive location of a Cisco lightweight access point, use the **config ap location** command.

config ap location *location cisco_ap*

Syntax Description

location	Location name of the access point (enclosed by double quotation marks).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

The following example shows how to configure the descriptive location for access point AP1:

```
(Cisco Controller) >config ap location "Building 1" AP1
```

config ap logging syslog level

To set the severity level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog level** command.

config ap logging syslog level *severity_level* {*cisco_ap* | **all**}

Syntax Description

severity_level	Severity levels are as follows: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7
cisco_ap	Cisco access point.
all	Specifies all access points.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the access point. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the access point.

This example shows how to set the severity for filtering syslog messages to 3:

```
(Cisco Controller) >config ap logging syslog level 3
```

config ap logging syslog facility

To set the facility level for filtering syslog messages for a particular access point or for all access points, use the **config ap logging syslog facility** command.

config ap logging syslog facility *facility-level* {*cisco_ap* | **all**}

Syntax Description

facility-level	Facility level is one of the following: • auth = Authorization system. • cron = Cron/at facility. • daemon = System daemons. • kern = Kernel. • local0 = Local use. • local1 = Local use. • local2 = Local use. • local3 = Local use. • local4 = Local use. • local5 = Local use. • local5 = Local use. • local6 = Local use. • local7 = Local use. • lpr = Line printer system. • mail = Mail system. • news = USENET news. • sys10 = System use. • sys11 = System use. • sys12 = System use. • sys13 = System use. • sys14 = System use. • sys9 = System use. • syslog = Syslog itself. • user = User process. • uucp Unix-to-Unix copy system.

cisco_ap	Configures for a specific access point.
all	Configures for all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to set the facility level for filtering syslog messages to auth for all access points:

```
(Cisco Controller) >config ap logging syslog facility auth all
```

config ap max-count

To configure the maximum number of access points supported by the controller, use the **config ap max-count** command.

config ap max-count *number*

Syntax Description

number	Number of access points supported by the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The access point count of the controller license overrides this count if the configured value is greater than the access point count of the license. A value of 0 indicates that there is no restriction on the maximum number of access points. If high availability is configured, you must reboot both the active and the standby controllers after you configure the maximum number of access points supported by the controller.

The following example shows how to configure the number of access points supported by the controller:

```
(Cisco Controller) >config ap max-count 100
```

config ap mgmtuser add

To configure username, password, and secret password for AP management, use the **config ap mgmtuser add** command.

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* {**all** | *cisco_ap*}

Syntax Description

username	Configures the username for AP management.
AP_username	Management username.
password	Configures the password for AP management.
AP_password	AP management password.
secret	Configures the secret password for privileged AP management.
secret	AP managemetn secret password.
all	Applies configuration to every AP that does not have a specific username.
cisco_ap	Cisco access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The following requirements are enforced on the password:

- The password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, and special characters.
- No character in the password can be repeated more than three times consecutively.
- The password sould not contain management username or reverse of usename.
- The password should not contain words like Cisco, oscic, admin, nimda or any variant obtained by changing the capitalization of letters by substituting 1, |, or ! or substituting 0 for o or substituting $ for s.

  The following requirement is enforced on the secret password:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

The following example shows how to add a username, password, and secret password for AP management:

```
(Cisco Controller) > config ap mgmtuser add username acd password Arc_1234 secret Mid_45
all
```

config ap mgmtuser delete

To force a specific access point to use the controller's global credentials, use the **config ap mgmtuser delete** command.

config ap mgmtuser delete *cisco_ap*

Syntax Description

cisco_ap	Access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the credentials of an access point:

```
(Cisco Controller) > config ap mgmtuser delete cisco_ap1
```

config ap mode

To change a controller communication option for an individual Cisco lightweight access point, use the **config ap mode** command.

config ap mode {**bridge** | **flexconnect submode** {**none** | **wips**} | **local submode** {**none** | **wips**} | **reap** | **rogue** | **sniffer** | **se-connect** | **monitor submode** {**none** | **wips**} |} *cisco_ap*

Syntax Description

bridge	Converts from a lightweight access point to a mesh access point (bridg
flexconnect	Enables FlexConnect mode on an access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonm lightweight access point (local mode).
reap	Enables remote edge access point mode on an access point.
rogue	Enables wired rogue detector mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.
se-connect	Enables flex+bridge mode on an access point.
flex+bridge	Enables spectrum expert mode on an access point.
submode	(Optional) Configures wIPS submode on an access point.
none	Disables the wIPS on an access point.
wips	Enables the wIPS submode on an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Local

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The sniffer mode captures and forwards all the packets from the clients on that channel to a remote machine that runs AiroPeek or other supported packet analyzer software. It includes information on the timestamp, signal strength, packet size and so on.

The following example shows how to set the controller to communicate with access point AP91 in bridge mode:

```
(Cisco Controller) > config ap mode bridge AP91
```

The following example shows how to set the controller to communicate with access point AP01 in local mode:

```
(Cisco Controller) > config ap mode local AP01
```

The following example shows how to set the controller to communicate with access point AP91 in remote office (REAP) mode:

```
(Cisco Controller) > config ap mode flexconnect AP91
```

The following example shows how to set the controller to communicate with access point AP91 in a wired rogue access point detector mode:

```
(Cisco Controller) > config ap mode rogue AP91
```

The following example shows how to set the controller to communicate with access point AP02 in wireless sniffer mode:

```
(Cisco Controller) > config ap mode sniffer AP02
```

config ap module3g

To configure the Cisco Universal Small Cell (USC) 8x18 Dual Mode Module, use the **config ap module3g** command.

config ap module3g {**enable** | **disable**} *ap-name*

Syntax Description

enable	Enables the Cisco USC 8x18 Dual Mode Module on the specified Cisco AP.
disable	Disables the Cisco USC 8x18 Dual Mode Module on the specified Cisco AP.
ap-name	Name of the Cisco AP **Note** In Release 8.1, only Cisco Aironet 3600I and 3700I APs are supported.

Command Default

Enabled

Command History

Release	Modification
8.1	This command was introduced.

Usage Guidelines

You might be prompted with a co-existence warning when Wi-Fi in 2.4-GHz and 3G/4G module are enabled.

This example shows how to enable Cisco USC 8x18 Dual Mode Module on a Cisco AP named *my-ap*

```
(Cisco Controller) >config ap module3g enable my-ap
```

config ap monitor-mode

To configure Cisco lightweight access point channel optimization, use the **config ap monitor-mode** command.

config ap monitor-mode {**802.11b fast-channel** | **no-optimization** | **tracking-opt** | **wips-optimized**} *cisco_ap*

Syntax Description

802.11b fast-channel	Configures 802.11b scanning channels for a monitor-mode access point.
no-optimization	Specifies no channel scanning optimization for the access point.
tracking-opt	Enables tracking optimized channel scanning for the access point.
wips-optimized	Enables wIPS optimized channel scanning for the access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
(Cisco Controller) > config ap monitor-mode wips-optimized AP01
```

config ap name

To modify the name of a Cisco lightweight access point, use the **config ap name** command.

config ap name *new_name old_name*

Syntax Description

new_name	Desired Cisco lightweight access point name.
old_name	Current Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify the name of access point AP1 to AP2:

```
(Cisco Controller) > config ap name AP1 AP2
```

config ap packet-dump

To configure the Packet Capture parameters on access points, use the **config ap packet-dump** command.

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**}}}

Syntax Description

buffer-size	Configures the buffer size for Packet Capture in the access point.
Size _in_KB	Size of the buffer. The range is from 1024 to 4096 KB.
capture-time	Configures the timer value for Packet Capture.
Time_in_Min	Timer value for Packet Capture. The range is from 1 to 60 minutes.
ftp	Configures FTP parameters for Packet Capture.
serverip	Configures the FTP server.
IP_addr	IP address of the FTP server.
path *path*	Configures FTP server path.
username *user_ID*	Configures the username for the FTP server.
password *password*	Configures the password for the FTP server.
start	Starts Packet Capture from the access point.
MAC_address	Client MAC Address for Packet Capture.
Cisco_AP	Name of the Cisco access point.
stop	Stops Packet Capture from the access point.
truncate	Truncates the packet to the specified length during Packet Capture.

Length_in_Bytes	Length of the packet after truncation. The range is from 20 to 1500.
classifier	Configures the classifier information for Packet Capture. You can specify the type of packets that needs to be captured.
arp	Captures ARP packets.
enable	Enables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, Inter Access Point Protocol (IAPP), IP, 802.11 management, or multicast packets.
disable	Disables capture of ARP, broadcast, 802.11 control, 802.11 data, dot1x, IAPP, IP, 802.11management, or multicast packets.
broadcast	Captures broadcast packets.
control	Captures 802.11 control packets.
data	Captures 802.11 data packets.
dot1x	Captures dot1x packets.
iapp	Captures IAPP packets.
ip	Captures IP packets.
management	Captures 802.11 management packets.
multicast	Captures multicast packets.
tcp	Captures TCP packets.
TCP_Port	TCP port number. The range is from 1 to 65535.
udp	Captures TCP packets.
UDP_Port	UDP port number. The range is from 1 to 65535.
ftp	Configures FTP parameters for Packet Capture.
server_ip	FTP server IP address.

Command Default

The default buffer size is 2 MB. The default capture time is 10 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.
8.8	This command is not supported for Cisco Wave 2 APs. For more information, see CSCvj19314.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as a beacon or probe response. Only packets that flow through the Radio driver in the Tx path will be captured.

Use the command **config ap packet-dump start** to start the Packet Capture from the access point. When you start Packet Capture, the controller sends a Control and Provisioning of Wireless Access Points protocol (CAPWAP) message to the access point to which the client is associated and captures packets. You must configure the FTP server and ensure that the client is associated to the access point before you start Packet Capture. If the client is not associated to the access point, you must specify the name of the access point.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to start Packet Capture from an access point:

```
(Cisco Controller) >config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

The following example shows how to capture 802.11 control packets from an access point:

```
(Cisco Controller) >config ap packet-dump classifier control enable
```

config ap port

To configure the port for a foreign access point, use the **config ap port** command.

config ap port *MAC port*

Syntax Description

MAC	Foreign access point MAC address.
port	Port number for accessing the foreign access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the port for a foreign access point MAC address:

```
(Cisco Controller) > config ap port 12:12:12:12:12:12 20
```

config ap power injector

To configure the power injector state for an access point, use the **config ap power injector** command.

config ap power injector {**enable** | **disable**} {*cisco_ap* | **all}** {**installed** | **override** | *switch_MAC*}

Syntax Description

enable	Enables the power injector state for an access point.
disable	Disables the power injector state for an access point.
cisco_ap	Name of the Cisco lightweight access point.
all	Specifies all Cisco lightweight access points connected to the controller.
installed	Detects the MAC address of the current switch port that has a power injector.
override	Overrides the safety checks and assumes a power injector is always installed.
switch_MAC	MAC address of the switch port with an installed power injector.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the power injector state for all access points:

```
(Cisco Controller) > config ap power injector enable all 12:12:12:12:12:12
```

config ap power pre-standard

To enable or disable the inline power Cisco pre-standard switch state for an access point, use the **config ap power pre-standard** command.

config ap power pre-standard {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the inline power Cisco pre-standard switch state for an access point.
disable	Disables the inline power Cisco pre-standard switch state for an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the inline power Cisco pre-standard switch state for access point AP02:

```
(Cisco Controller) > config ap power pre-standard enable AP02
```

config ap preferred-mode

To configure the preferred mode, use the **config ap preferred-mode** command.

config appreferred-mode { **ipv4** | **ipv6** | **any** } { *AP_name* | *Ap-group_name* | *all* }

Syntax Description

ipv4	Configures IPv4 as the preferred mode
ipv6	Configures IPv6 as the preferred mode
any	Configures any as the preferred mode
AP_name	Configures the preferred mode to the AP
Ap-group_name	Configures the preferred mode to the AP group members
all	Configures the preferred mode to all the APs

Command Default

None

Command History

Release	Modification
8.0	This command was introduced. It supports both IPv4 and IPv6.

Example

The following example shows how to configure IPv6 as the preferred mode to lightweight access point AP1

```
(Cisco Controller) >config ap preferred-mode ipv6 AP1
```

config ap primary-base

To set the Cisco lightweight access point primary controller, use the **config ap primary-base** command.

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

Syntax Description

controller_name	Name of the controller.
Cisco_AP	Cisco lightweight access point name.
controller_ip_address	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to set an access point primary controller IPv4 address for an Cisco AP:

```
(Cisco Controller) > config ap primary-base SW_1 AP2 10.0.0.0
```

The following example shows how to set an access point primary controller IPv6 address for an Cisco AP:

```
(Cisco Controller) > config ap primary-base SW_1 AP2 2001:DB8:0:1::1
```

Related Commands

show ap config general

config ap priority

To assign a priority designation to an access point that allows it to reauthenticate after a controller failure by priority rather than on a first-come-until-full basis, use the **config ap priority** command.

config ap priority {**1** | **2** | **3** | **4**} *cisco_ap*

Syntax Description

1	Specifies low priority.
2	Specifies medium priority.
3	Specifies high priority.
4	Specifies the highest (critical) priority.
cisco_ap	Cisco lightweight access point name.

Command Default

1 - Low priority.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In a failover situation, if the backup controller does not have enough ports to allow all the access points in the affected area to reauthenticate, it gives priority to higher-priority access points over lower-priority ones, even if it means replacing lower-priority access points.

The following example shows how to assign a priority designation to access point AP02 that allows it to reauthenticate after a controller failure by assigning a reauthentication priority 3:

```
(Cisco Controller) > config ap priority 3 AP02
```

config ap reporting-period

To reset a Cisco lightweight access point, use the **config ap reporting-period** command.

config ap reporting-period *period*

Syntax Description

period	Time period in seconds between 10 and 120.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset an access point reporting period to 120 seconds:

```
> config ap reporting-period 120
```

config ap reset

To reset a Cisco lightweight access point, use the **config ap reset** command.

config ap reset *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset an access point:

```
(Cisco Controller) > config ap reset AP2
```

config ap retransmit interval

To configure the access point control packet retransmission interval, use the **config ap retransmit interval** command.

config ap retransmit interval *seconds* {**all** | *cisco_ap*}

Syntax Description

seconds	AP control packet retransmission timeout between 2 and 5 seconds.
all	Specifies all access points.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the retransmission interval for all access points globally:

```
(Cisco Controller) > config ap retransmit interval 4 all
```

config ap retransmit count

To configure the access point control packet retransmission count, use the **config ap retransmit count** command.

config ap retransmit count *count* {**all** | *cisco_ap*}

Syntax Description

count	Number of times control packet will be retransmitted. The range is from 3 to 8.
all	Specifies all access points.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the retransmission retry count for a specific access point:

```
(Cisco Controller) > config ap retransmit count 6 cisco_ap
```

config ap role

To specify the role of an access point in a mesh network, use the **config ap role** command.

config ap role {**rootAP** | **meshAP**} *cisco_ap*

Syntax Description

rootAP	Designates the mesh access point as a root access point (RAP).
meshAP	Designates the mesh access point as a mesh access point (MAP).
cisco_ap	Name of the Cisco lightweight access point.

Command Default

meshAP.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **meshAP** keyword if the access point has a wireless connection to the controller, or use the **rootAP** keyword if the access point has a wired connection to the controller. If you change the role of the AP, the AP will be rebooted.

The following example shows how to designate mesh access point AP02 as a root access point:

```
(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

To configure the Reset button for an access point, use the **config ap rst-button** command.

config ap rst-button {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the Reset button for an access point.
disable	Disables the Reset button for an access point.
cisco_ap	Name of the Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Reset button for access point AP03:

```
(Cisco Controller) > config ap rst-button enable AP03
```

config ap secondary-base

To set the Cisco lightweight access point secondary controller, use the **config ap secondary-base** command.

config ap secondary-base *Controller_name Cisco_AP* [*Controller_IP_address*]

Syntax Description

controller_name	Name of the controller.
Cisco_AP	Cisco lightweight access point name.
Controller_IP_address	(Optional). If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to set an access point secondary controller:

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 10.0.0.0
```

The following example shows how to set an access point primary controller IPv6 address for an Cisco AP:

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 2001:DB8:0:1::1
```

Related Commands

show ap config general

config ap sniff

To enable or disable sniffing on an access point, use the **config ap sniff** command.

config ap sniff { **802.11a** | **802.11b** } { **enable** *channel server_ip* | **disable** } *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
enable	Enables sniffing on an access point.
channel	Channel to be sniffed.
server_ip	IP address of the remote machine running Omnipeek, Airopeek,AirMagnet, or Wireshark software.
disable	Disables sniffing on an access point.
cisco_ap	Access point configured as the sniffer.

Command Default

Channel 36.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When the sniffer feature is enabled on an access point, it starts sniffing the signal on the given channel. It captures and forwards all the packets to the remote computer that runs Omnipeek, Airopeek, AirMagnet, or Wireshark software. It includes information on the timestamp, signal strength, packet size and so on.

Before an access point can act as a sniffer, a remote computer that runs one of the listed packet analyzers must be set up so that it can receive packets sent by the access point. After the Airopeek installation, copy the following .dll files to the location where airopeek is installed:

- socket.dll file to the Plug-ins folder (for example, C:\Program Files\WildPackets\AiroPeek\Plugins)
- socketres.dll file to the PluginRes folder (for example, C:\Program Files\WildPackets\AiroPeek\1033\PluginRes)

The following example shows how to enable the sniffing on the 802.11a an access point from the primary controller:

```
(Cisco Controller) > config ap sniff 80211a enable 23 11.22.44.55 AP01
```

config ap ssh

To enable Secure Shell (SSH) connectivity on an access point, use the **config ap ssh** command.

config ap ssh {**enable** | **disable** | **default**} *cisco_ap* | *all*

Syntax Description

enable	Enables the SSH connectivity on an access point.
disable	Disables the SSH connectivity on an access point.
default	Replaces the specific SSH configuration of an access point with the global SSH configuration.
cisco_ap	Cisco access point name.
all	All access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco wireless LAN controller for all network operation and in the event of a hardware reset.

The following example shows how to enable SSH connectivity on access point Cisco_ap2:

```
> config ap ssh enable cisco_ap2
```

config ap static-ip

To configure Static IP address settings on Cisco lightweight access point , use the **config ap static-ip** command.

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**}}

Syntax Description

enable	Enables the Cisco lightweight access point static IP address.
disable	Disables the Cisco lightweight access point static IP address. The access point uses DHCP to get the IP address.
Cisco_AP	Cisco lightweight access point name.
AP_IP_addr	Cisco lightweight access point IP address
IP_netmask/prefix_length	Cisco lightweight access point network mask.
gateway	IP address of the Cisco lightweight access point gateway.
add	Adds a domain or DNS server.
domain	Specifies the domain to which a specific access point or all access points belong.
all	Specifies all access points.
domain_name	Specifies a domain name.
nameserver	Specifies a DNS server so that a specific access point or all access points can discover the controller using DNS resolution.
nameserver-ip	DNS server IP address.
delete	Deletes a domain or DNS server.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

An access point cannot discover the controller using Domain Name System (DNS) resolution if a static IP address is configured for the access point, unless you specify a DNS server and the domain to which the access point belongs.

After you enter the IPv6 address, Prefix-length and IPv6 gateway address, the CAPWAP tunnel will restart for access point. Changing the AP's IP address will cause the AP to disjoin. After the access point rejoins the controller, you can enter the domain and IPv6 DNS server information.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure static IP address on an access point:

```
(Cisco Controller) >config ap static-ip enable AP2 209.165.200.225 255.255.255.0
209.165.200.254
```

The following example shows how to configure static IPv6 address on an access point:

```
(Cisco Controller) > config ap static-ip enable AP2 2001:DB8:0:1::1
```

Related Commands

show ap config general

config ap stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco wireless LAN controller, use the **config ap stats-timer** command.

config ap stats-timer *period cisco_ap*

Syntax Description

period	Time in seconds from 0 to 65535. A zero value disables the timer.
cisco_ap	Cisco lightweight access point name.

Command Default

The default value is 0 (disabled state).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A value of 0 (zero) means that the Cisco lightweight access point does not send any DOT11 statistics. The acceptable range for the timer is from 0 to 65535 seconds, and the Cisco lightweight access point must be disabled to set this value.

The following example shows how to set the stats timer to 600 seconds for access point AP2:

```
(Cisco Controller) > config ap stats-timer 600 AP2
```

config ap syslog host global

To configure a global syslog server for all access points that join the controller, use the **config ap syslog host global** command.

config ap syslog host global *ip_address*

Syntax Description

ip_address	IPv4/IPv6 address of the syslog server.

Command Default

The default value of the IPv4 address of the syslog server is 255.255.255.255.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

By default, the global syslog server IP address for all access points is 255.255.255.255. Make sure that the access points can reach the subnet on which the syslog server resides before configuring the syslog server on the controller. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a global syslog server, using IPv4 address, for all access points:

```
(Cisco Controller) > config ap syslog host global 255.255.255.255
```

The following example shows how to configure a global syslog server, using IPv6 address, for all access points:

```
(Cisco Controller) > config ap syslog host global  2001:9:10:56::100
```

config ap syslog host specific

To configure a syslog server for a specific access point, use the **config ap syslog host specific** command.

config ap syslog host specific *ap_nameip_address*

Syntax Description

ap_name	Cisco lightweight access point.
ip_address	IPv4/IPv6 address of the syslog server.

Command Default

The default value of the syslog server IP address is 0.0.0.0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

By default, the syslog server IP address for each access point is 0.0.0.0, indicating that it is not yet set. When the default value is used, the global access point syslog server IP address is pushed to the access point.

This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a syslog server:

```
(Cisco Controller) >config ap syslog host specific 0.0.0.0
```

The following example shows how to configure a syslog server for a specific AP, using IPv6 address:

```
(Cisco Controller) > config ap syslog host specific AP3600 2001:9:10:56::100
```

config ap tcp-mss-adjust

To enable or disable the TCP maximum segment size (MSS) on a particular access point or on all access points, use the **config ap tcp-mss-adjust** command.

config ap tcp-mss-adjust {**enable** | **disable**} {*cisco_ap* | **all**} *size*

Syntax Description

enable	Enables the TCP maximum segment size on an access point.
disable	Disables the TCP maximum segment size on an access point.
cisco_ap	Cisco access point name.
all	Specifies all access points.
size	Maximum segment size. • IPv4—Specify a value between 536 and 1363. • IPv6—Specify a value between 1220 and 1331. **Note** Any TCP MSS value that is below 1220 and above 1331 will not be effective for CAPWAP v6 AP.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv6.

Usage Guidelines

When you enable this feature, the access point checks for TCP packets to and from wireless clients in its data path. If the MSS of these packets is greater than the value that you configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the new configured value.

This example shows how to enable the TCP MSS on access point cisco_ap1 with a segment size of 1200 bytes:

```
(Cisco Controller) > config ap tcp-mss-adjust enable cisco_ap1 1200
```

config ap telnet

To enable Telnet connectivity on an access point, use the **config ap telnet** command.

config ap telnet { **enable** | **disable** | **default** } *cisco_ap* | *all*

Syntax Description

enable	Enables the Telnet connectivity on an access point.
disable	Disables the Telnet connectivity on an access point.
default	Replaces the specific Telnet configuration of an access point with the global Telnet configuration.
cisco_ap	Cisco access point name.
all	All access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

- The Cisco lightweight access point associates with this controller for all network operation and in the event of a hardware reset.
- Telnet is not supported on Cisco Aironet 1810 OEAP, 1810W, 1830, 1850, 2800, and 3800 Series APs.

The following example shows how to enable Telnet connectivity on access point cisco_ap1:

```
(Cisco Controller) >config ap telnet enable cisco_ap1
```

The following example shows how to disable Telnet connectivity on access point cisco_ap1:

```
(Cisco Controller) > config ap telnet disable cisco_ap1
```

config ap tertiary-base

To set the Cisco lightweight access point tertiary controller, use the **config ap tertiary-base** command.

config ap tertiary-base *controller_name Cisco_AP* [*controller_ip_address*]

Syntax Description

controller_name	Name of the controller.
Cisco_AP	Cisco lightweight access point name.
controller_ip_address	(Optional) If the backup controller is outside the mobility group to which the access point is connected, then you need to provide the IP address of the primary, secondary, or tertiary controller. **Note** For OfficeExtend access points, you must enter both the name and IP address of the controller. Otherwise, the access point cannot join this controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

OfficeExtend access points do not use the generic broadcast or over-the air (OTAP) discovery process to find a controller. You must configure one or more controllers because OfficeExtend access points try to connect only to their configured controllers.

The Cisco lightweight access point associates with this controller for all network operations and in the event of a hardware reset.

This command supports both IPv4 and IPv6 address formats.

This example shows how to set the access point tertiary controller:

```
(Cisco Controller) > config ap tertiary-base SW_1 AP02 10.0.0.0
```

The following example shows how to set an access point tertiary controller IPv6 address for an Cisco AP:

```
(Cisco Controller) > config ap tertiary-base SW_1 AP2 2001:DB8:0:1::1
```

Related Commands

show ap config general

config ap tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **config ap ftp-downgrade** command.

config ap tftp-downgrade *tftp_ip_addressfilename Cisco_AP*

Syntax Description

tftp_ip_address	IP address of the TFTP server.
filename	Filename of the access point image file on the TFTP server.
Cisco_AP	Access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the settings for downgrading access point ap1240_102301:

```
(Cisco Controller) >config ap ftp-downgrade 209.165.200.224 1238.tar ap1240_102301
```

config ap username

To assign a username and password to access either a specific access point or all access points, use the **config ap username** command.

config ap username *user_id* **password** *passwd* [**all** | *ap_name*]

Syntax Description

user_id	Administrator username.
passwd	Administrator password.
all	(Optional) Specifies all access points.
ap_name	Name of a specific access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to assign a username and password to a specific access point:

```
(Cisco Controller) > config ap username jack password blue la204
```

The following example shows how to assign the same username and password to a all access points:

```
(Cisco Controller) > config ap username jack password blue all
```

config ap venue

To configure the venue information for 802.11u network on an access point, use the **config ap venue** command.

config ap venue {**add***venue_name venue-group venue-type lang-code cisco-ap* | **delete**}

Syntax Description

add	Adds venue information.
venue_name	Venue name.
venue_group	Venue group category. See the table below for details on venue group mappings.
venue_type	Venue type. This value depends on the venue-group specified. See the table below for venue group mappings.
lang_code	Language used. An ISO-14962-1997 encoded string that defines the language. This string is a three character language code. Enter the first three letters of the language in English (for example, eng for English).
cisco_ap	Name of the access point.
deletes	Deletes venue information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the venue details for an access point named cisco-ap1:

```
(Cisco Controller) > config ap venue add test 11 34 eng cisco-ap1
```

This table lists the different venue types for each venue group.

Table 5: Venue Group Mapping

Venue Group Name	Value	Venue Type for Group
UNSPECIFIED	0	

Venue Group Name	Value	Venue Type for Group
ASSEMBLY	1	• 0—UNSPECIFIED ASSEMBLY • 1—ARENA • 2—STADIUM • 3—PASSENGER TERMINAL (E.G., AIRPORT, BUS, FERRY, TRAIN STATION) • 4—AMPHITHEATER • 5—AMUSEMENT PARK • 6—PLACE OF WORSHIP • 7—CONVENTION CENTER • 8—LIBRARY • 9—MUSEUM • 10—RESTAURANT • 11—THEATER • 12—BAR • 13—COFFEE SHOP • 14—ZOO OR AQUARIUM • 15—EMERGENCY COORDINATION CENTER
BUSINESS	2	• 0—UNSPECIFIED BUSINESS • 1—DOCTOR OR DENTIST OFFICE • 2—BANK • 3—FIRE STATION • 4—POLICE STATION • 6—POST OFFICE • 7—PROFESSIONAL OFFICE • 8—RESEARCH AND DEVELOPMENT FACILITY • 9—ATTORNEY OFFICE

Venue Group Name	Value	Venue Type for Group
EDUCATIONAL	3	• 0—UNSPECIFIED EDUCATIONAL • 1—SCHOOL, PRIMARY • 2—SCHOOL, SECONDARY • 3—UNIVERSITY OR COLLEGE
FACTORY-INDUSTRIAL	4	• 0—UNSPECIFIED FACTORY AND INDUSTRIAL • 1—FACTORY
INSTITUTIONAL	5	• 0—UNSPECIFIED INSTITUTIONAL • 1—HOSPITAL • 2—LONG-TERM CARE FACILITY (E.G., NURSING HOME, HOSPICE, ETC.) • 3—ALCOHOL AND DRUG RE-HABILITATION CENTER • 4—GROUP HOME • 5—PRISON OR JAIL
MERCANTILE	6	• 0—UNSPECIFIED MERCANTILE • 1—RETAIL STORE • 2—GROCERY MARKET • 3—AUTOMOTIVE SERVICE STATION • 4—SHOPPING MALL • 5—GAS STATION
RESIDENTIAL	7	• 0—UNSPECIFIED RESIDENTIAL • 1—PRIVATE RESIDENCE • 2—HOTEL OR MOTEL • 3—DORMITORY • 4—BOARDING HOUSE
STORAGE	8	UNSPECIFIED STORAGE

Venue Group Name	Value	Venue Type for Group
UTILITY-MISC	9	0—UNSPECIFIED UTILITY AND MISCELLANEOUS
VEHICULAR	10	• 0—UNSPECIFIED VEHICULAR • 1—AUTOMOBILE OR TRUCK • 2—AIRPLANE • 3—BUS • 4—FERRY • 5—SHIP OR BOAT • 6—TRAIN • 7—MOTOR BIKE
OUTDOOR	11	• 0—UNSPECIFIED OUTDOOR • 1—MUNI-MESH NETWORK • 2—CITY PARK • 3—REST AREA • 4—TRAFFIC CONTROL • 5—BUS STOP • 6—KIOSK

config ap wlan

To enable or disable wireless LAN override for a Cisco lightweight access point radio, use the **config ap wlan** command.

config ap wlan {**enable** | **disable**} {**802.11a** | **802.11b**} *wlan_id cisco_ap*

Syntax Description

enable	Enables the wireless LAN override on an access point.
disable	Disables the wireless LAN override on an access point.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
wlan_id	Cisco wireless LAN controller ID assigned to a wireless LAN.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable wireless LAN override on the AP03 802.11a radio:

```
(Cisco Controller) > config ap wlan 802.11a AP03
```

config atf 802.11

Configure Cisco Air Time Fairness at the network level, at an AP group level, or at an AP radio level by using the **config atf 802.11** command.

config atf 802.11 {**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} {[*ap-group-name*] | [*ap-name*]}} | {**optimization** {**enable** | **disable**}}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b/g network settings
mode	Configures the granularity of Cisco ATF enforcement
disable	Disables Cisco ATF
monitor	Configures Cisco ATF in monitor mode
enforce-policy	Configures Cisco ATF in enforcement mode
optimization	Configures airtime optimization
enable	Enables airtime optimization
disable	Disabled airtime optimization

Command History

Release	Modification
8.1	This command was introduced

- To configure Cisco ATF in monitor mode on an 802.11a network, enter this command:

```
(Cisco Controller) >config atf 802.11a mode monitor
```

- To enable airtime optimization on an 802.11a network, enter this command:

```
(Cisco Controller) >config atf 802.11a optimization enable
```

config atf policy

To configure Cisco Air Time Fairness (ATF) policies, use the **config atf policy** command.

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*}}

Syntax Description

create	Creates an air time policy
modify	Modifies an air time policy
delete	Deletes an air time policy
client-sharing {**enable** | **disable** *policy-name*}	Enables or disables client fair sharing for the specified policy name
policy-id	Policy ID between 1 and 511
policy-name	Name of the Cisco ATF policy
policy-weight	Policy weight between 5 and 100

Command History

Release	Modification
8.1.122.0	This command was introduced
8.2	**client-sharing** {**enable** | **disable**} option was added.

This example shows how to create a Cisco ATF policy:

```
(Cisco Controller) >config atf policy create 2 test-policy 70
```

config auth-list add

To create an authorized access point entry, use the **config auth-list add** command.

config auth-list add {**mic** | **ssc**} *AP_MAC* [*AP_key*]

Syntax Description

mic	Specifies that the access point has a manufacture-installed certificate.
ssc	Specifies that the access point has a self-signed certificate.
AP_MAC	MAC address of a Cisco lightweight access point.
AP_key	(Optional) Key hash value that is equal to 20 bytes or 40 digits.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create an authorized access point entry with a manufacturer-installed certificate on MAC address 00:0b:85:02:0d:20:

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

Related Commands

config auth-list delete

config auth-list ap-policy

config auth-list ap-policy

To configure an access point authorization policy, use the **config auth-list ap-policy** command.

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **ssc** {**enable** | **disable**}}

Syntax Description

authorize-ap enable	Enables the authorization policy.
authorize-ap disable	Disables the AP authorization policy.
ssc enable	Allows the APs with self-signed certificates to connect.
ssc disable	Disallows the APs with self-signed certificates to connect.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an access point authorization policy:

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

The following example shows how to enable an access point with a self-signed certificate to connect:

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

Related Commands

config auth-list delete

config auth-list add

config auth-list delete

To delete an access point entry, use the **config auth-list delete** command.

config auth-list delete *AP_MAC*

Syntax Description

AP_MAC	MAC address of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an access point entry for MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

Related Commands

config auth-list delete

config auth-list add

config auth-list ap-policy

config avc profile create

To create a new Application Visibility and Control (AVC) profile, use the **config avc profile create** command.

config avc profile *profile_name* **create**

Syntax Description

profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
create	Creates a new AVC profile.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs. You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN.

The following example shows how to create a new AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 create
```

Related Commands

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

To delete an Application Visibility and Control (AVC) profile, use the **config avc profile delete** command.

config avc profile *profile_name* **delete**

Syntax Description

profile_name	Name of the AVC profile.
delete	Deletes an AVC profile.

Command Default

The AVC profile is not deleted.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to delete an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 delete
```

Related Commands

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

To configure a rule for an Application Visibility and Control (AVC) profile, use the **config avc profile rule** command.

config avc profile *profile_name* **rule** {**add** | **remove**} **application** *application_name* {**drop** | **mark** *dscp*}

Syntax Description

profile_name	Name of the AVC profile.
rule	Configures a rule for the AVC profile.
add	Creates a rule for the AVC profile.
remove	Deletes a rule for the AVC profile.
application	Specifies the application that has to be dropped or marked.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
drop	Drops the upstream and downstream packets that correspond to the chosen application.
mark	Marks the upstream and downstream packets that correspond to the chosen application with the Differentiated Services Code Point (DSCP) value that you specify in the drop-down list. The DSCP value helps you provide differentiated services based on the QoS levels.
dscp	Packet header code that is used to define the QoS across the Internet. The range is from 0 to 63.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to configure a rule for an AVC profile:

```
(Cisco Controller) > config avc profile avcprofile1 rule add application gmail mark 10
```

Related Commands

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

To set the band select probe cycle count, use the **config band-select cycle-count** command.

config band-select cycle-count *count*

Syntax Description

count	Value for the cycle count between 1 to 10.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the probe cycle count for band select to 8:

```
(Cisco Controller) > config band-select cycle-count 8
```

Related Commands

config band-select cycle-threshold

config band-select expire

config band-select client-rssi

config band-select cycle-threshold

To set the time threshold for a new scanning cycle, use the **config band-select cycle-threshold** command.

config band-select cycle-threshold *threshold*

Syntax Description

threshold	Value for the cycle threshold between 1 and 1000 milliseconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
(Cisco Controller) > config band-select cycle-threshold 700
```

Related Commands

config band-select cycle-count

config band-select expire

config band-select client-rssi

config band-select expire

To set the entry expire for band select, use the **config band-select expire** command.

config band-select expire {**suppression** | **dual-band**} *seconds*

Syntax Description

suppression	Sets the suppression expire to the band select.
dual-band	Sets the dual band expire to the band select.
seconds	• Value for suppression between 10 to 200 seconds. • Value for a dual-band between 10 to 300 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the suppression expire to 70 seconds:

```
(Cisco Controller) > config band-select expire suppression 70
```

Related Commands

config band-select cycle-threshold

config band-select client-rssi

config band-select cycle-count

config band-select client-rssi

To set the client received signal strength indicator (RSSI) threshold for band select, use the **config band-select client-rssi** command.

config band-select client-rssi *rssi*

Syntax Description

rssi	Minimum dBM of a client RSSI to respond to probe

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the RSSI threshold for band select to 70:

```
(Cisco Controller) > config band-select client-rssi 70
```

Related Commands

config band-select cycle-threshold

config band-select expire

config band-select cycle-count

config boot

To change a Cisco wireless LAN controller boot option, use the **config boot** command.

config boot {**primary** | **backup**}

Syntax Description

primary	Sets the primary image as active.
backup	Sets the backup image as active.

Command Default

The default boot option is **primary**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Each Cisco wireless LAN controller can boot off the primary, last-loaded operating system image (OS) or boot off the backup, earlier-loaded OS image.

The following example shows how to set the primary image as active so that the LAN controller can boot off the primary, last loaded image:

```
(Cisco Controller) > config boot primary
```

The following example shows how to set the backup image as active so that the LAN controller can boot off the backup, earlier loaded OS image:

```
(Cisco Controller) > config boot backup
```

Related Commands

show boot

config call-home contact email address

To configure the call-home contact email address, use the **config call-home contact-email-addr** command.

config call-home contact-email-addr *email-address*

Syntax Description

email-address	call-home contact email address

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to add call-home contact email address:

```
(Cisco Controller) >config call-home contact-email-addr device1@example1.com
```

config call-home events

To enable or disable the call-home event reporting, use the **call-home events** command.

config call-home events {**enable** | **disable**}

Syntax Description

enable	Enables the call-home event reporting.
disable	Disables the call-home event reporting.

Command Default

Enable

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to disable call-home event reporting:

```
(Cisco Controller) > config call-home events disable
```

config call-home http-proxy ipaddr

To configure the http proxy address for reporting, use the **config call-home http-proxy ipaddr** command.

config call-home http-proxy ipaddr *ip-address* **port** *port*

Syntax Description

ip-address	the http-proxy IP address
port	the http-proxy port number

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to configure call home with the http-proxy IP address:

```
(Cisco Controller) >config call-home http-proxy ipaddr 209.165.200.224 port 773
```

config call-home http-proxy ipaddr 0.0.0.0

To reset the http proxy settings for reporting, use the **config call-home http-proxy ipaddr 0.0.0.0** command.

config call-home http-proxy ipaddr *0.0.0.0*

Syntax Description

0.0.0.0	resets the http-proxy settings

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to reset call home http-proxy settings:

```
(Cisco Controller) >config call-home http-proxy ipaddr 0.0.0.0
```

config call-home profile

To create, update the call-home profile, use the **config call-home profile** command.

config call-home profile {**create** | **update** } *profile-name* {**sm-license-data** | **all** | **call-home-data**} {**short-text** | **long-text** | **xml** } *url*

Syntax Description

create	create a Call-Home profile
update	updates a Call-Home profile
sm-license-data	Configures Smart license reporting profile
all	Configures reporting profile for all modules
call-home-data	Configures call home data reporting profile
short-text	Configures data reporting in short-text format
long-text	Configures data reporting in long-text format
xml	Configures data reporting in XML format
url	url name

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to create a xml format reporting Call-Home profile:

```
(Cisco Controller) > config call-home profile create example-profile sm-license-data xml
internal.example.com
```

config call-home profile delete

To delete the call-home profile, use the **config call-home profile delete** command.

config call-home profile delete *profile-name*

Syntax Description

profile-name	Call-Home profile to be deleted.

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to delete a Call-Home profile:

```
(Cisco Controller) > config call-home profile delete example-profile
```

config call-home profile status

To enable or disable the user profile, use the **config call-home profile status** command.

config call-home profile status {**enable** | **disable**}

Syntax Description

enable	enables the status of call-home profile
disable	disables the status of call-home profile

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to disable a Call-Home profile:

```
(Cisco Controller) >config call-home profile status disable
```

config call-home reporting

To set the privacy level for data reporting, use the **config call-home reporting data-privacy level** command.

config call-home reporting data-privacy level {**normal** | **high**} **hostname** *host name*

Syntax Description

normal	scrubs all normal-level commands
high	scrubs all normal-level commands, the IP domain name ar
hostname	scrubs all high-level commands plus the hostname comma

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to configure normal privacy level:

```
(Cisco Controller) >config call-home reporting data-privacy- level normal hostname
internal.example.com
```

config call-home tac-profile

To enable or disable the tac-profile, use the **config call-home tac-profile status** command.

config call-home tac-profile status { **enable** | **disable** }

Syntax Description

enable	enables call-home TAC profile.
disable	disables call-home TAC profile.

Command Default

Enable

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to disable call home tac-profile:

```
(Cisco Controller) >config call-home tac-profile status disable
```

config cdp

To configure the Cisco Discovery Protocol (CDP) on the controller, use the **config cdp** command.

config cdp {**enable** | **disable** | **advertise-v2** {**enable** | **disable**} | **timer***seconds* | **holdtime** *holdtime_interval*}

Syntax Description

enable	Enables CDP on the controller.
disable	Disables CDP on the controller.
advertise-v2	Configures CDP version 2 advertisements.
timer	Configures the interval at which CDP messages are t be generated.
seconds	Time interval at which CDP messages are to be generated. The range is from 5 to 254 seconds.
holdtime	Configures the amount of time to be advertised as the time-to-live value in generated CDP packets.
holdtime_interval	Maximum hold timer value. The range is from 10 to 2 seconds.

Command Default

The default value for CDP timer is 60 seconds.

The default value for CDP holdtime is 180 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the CDP maximum hold timer to 150 seconds:

```
(Cisco Controller) > config cdp timer 150
```

Related Commands

config ap cdp

show cdp

show ap cdp

config certificate

To configure Secure Sockets Layer (SSL) certificates, use the **config certificate** command.

config certificate {**generate** {**csr-webadmin** | **csr-webauth** | **webadmin** | **webauth**}

Syntax Description

generate	Specifies authentication certificate generation settings.
csr-webadmin	Generates a new web administration certificate signing req
csr-webauth	Generates a new web authentication signing request
webadmin	Generates a new web administration certificate.
webauth	Generates a new web authentication certificate.

Command Default

None

Usage Guidelines

With all parameters in CSR aligned with RFC-5280, there are some restrictions as follows:

- *emailAddress* in CSR can only be 128 characters long.
- If the CSR is generated using the CLI, the maximum number of characters (of all input combined for CSR) is limited to 500 including **config certificate generate csr-*****.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced with new keywords in Release 8.3.

The following example shows how to generate a new web administration SSL certificate:

```
(Cisco Controller) > config certificate generate webadmin
Creating a certificate may take some time. Do you wish to continue? (y/n)
```

config certificate lsc

To configure Locally Significant Certificate (LSC) certificates, use the **config certificate lsc** command.

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*}

Syntax Description

enable	Enables LSC certificates on the controller.
disable	Disables LSC certificates on the controller.
ca-server	Specifies the Certificate Authority (CA) server settings.
http://url:port/path	Domain name or IP address of the CA server.
ca-cert	Specifies CA certificate database settings.
add	Obtains a CA certificate from the CA server and adds it to the controller's certificate database.
delete	Deletes a CA certificate from the controller's certificate database.
subject-params	Specifies the device certificate settings.
country state city orgn dept email	Country, state, city, organization, department, and email of the certificate authority. **Note** The common name (CN) is generated automatically on the access point using the current MIC/SSC format *Cxxxx-MacAddr*, where *xxxx* is the product number.
other-params	Specifies the device certificate key size settings.
keysize	Value from 384 to 2048 (in bits); the default value is 2048.
ap-provision	Specifies the access point provision list settings.
auth-list	Specifies the provision list authorization settings.
ap_mac	MAC address of access point to be added or deleted from the provision list.
revert-cert	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate.
retries	Value from 0 to 255; the default value is 3. **Note** If you set the number of retries to 0 and the access point fails to join the controller using an LSC, the access point does not attempt to join the controller using the default certificate. If you are configuring LSC for the first time, we recommend that you configure a nonzero value.

Command Default

The default value of *keysize* is 2048 bits. The default value of *retries* is 3.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure only one CA server. To configure a different CA server, delete the configured CA server by using the **config certificate lsc ca-server delete** command, and then configure a different CA server.

If you configure an access point provision list, only the access points in the provision list are provisioned when you enable AP provisioning (in Step 8). If you do not configure an access point provision list, all access points with an MIC or SSC certificate that join the controller are LSC provisioned.

The following example shows how to enable the LSC settings:

```
(Cisco Controller) >config certificate lsc enable
```

This example shows how to enable the LSC settings for Certificate Authority (CA) server settings:

```
(Cisco Controller) >config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

The following example shows how to add a CA certificate from the CA server and add it to the controller's certificate database:

```
(Cisco Controller) >config certificate lsc ca-cert add
```

The following example shows how to configure an LSC certificate with the keysize of 2048 bits:

```
(Cisco Controller) >config certificate lsc keysize 2048
```

config certificate ssc

To configure Self Signed Certificates (SSC) certificates, use the **config certificate ssc** command.

config certificate ssc hash validation {**enable** | **disable**}

Syntax Description

hash	Configures the SSC hash key.
validation	Configures hash validation of the SSC certificate.
enable	Enables hash validation of the SSC certificate.
disable	Disables hash validation of the SSC certificate.

Command Default

The SSC certificate is enabled by default..

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable the SSC hash validation, an AP validates the SSC certificate of the virtual controller. When an AP validates the SSC certificate, it checks if the hash key of the virtual controller matches the hash key stored in its flash. If a match is found, the validation passes and the AP moves to the Run state. If a match is not found, the validation fails and the AP disconnects from the controller and restarts the discovery process. By default, hash validation is enabled. Hence, an AP must have the virtual controller hash key in its flash before associating with the virtual controller. If you disable hash validation of the SSC certificate, the AP bypasses the hash validation and directly moves to the Run state.

APs can associate with a physical controller, download the hash keys and then associate with a virtual controller. If the AP is associated to a physical controller and if hash validation is disabled, it joins any virtual controller without hash validation.

The following example shows how to enable hash validation of the SSC certificate:

```
(Cisco Controller) > config certificate ssc hash validation enable
```

Related Commands

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

To use a device certificate for web administration, use the **config certificate use-device-certificate webadmin** command.

config certificate use-device-certificate webadmin

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to use a device certificate for web administration:

```
(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.
```

Related Commands

config certificate

show certificate compatibility

show certificate lsc

show certificate ssc

show certificate summary

show local-auth certificates

config client ccx clear-reports

To clear the client reporting information, use the **config client ccx clear-reports** command.

config client ccx clear-reports *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) >config client ccx clear-reports 00:1f:ca:cf:b6:60
```

config client ccx clear-results

To clear the test results on the controller, use the **config client ccx clear-results** command.

config client ccx clear-results *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to clear the test results of the client MAC address 00:1f:ca:cf:b6:60:

```
(Cisco Controller) >config client ccx clear-results 00:1f:ca:cf:b6:60
```

config client ccx default-gw-ping

To send a request to the client to perform the default gateway ping test, use the **config client ccx default-gw-ping** command.

config client ccx default-gw-ping *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

The following example shows how to send a request to the client00:0b:85:02:0d:20 to perform the default gateway ping test:

```
(Cisco Controller) >config client ccx default-gw-ping 00:0b:85:02:0d:20
```

config client ccx dhcp-test

To send a request to the client to perform the DHCP test, use the **config client ccx dhcp-test** command.

config client ccx dhcp-test *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

The following example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DHCP test:

```
(Cisco Controller) >config client ccx dhcp-test 00:E0:77:31:A3:55
```

config client ccx dns-ping

To send a request to the client to perform the Domain Name System (DNS) server IP address ping test, use the **config client ccx dns-ping** command.

config client ccx dns-ping *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

The following example shows how to send a request to a client to perform the DNS server IP address ping test:

```
(Cisco Controller) >config client ccx dns-ping 00:E0:77:31:A3:55
```

config client ccx dns-resolve

To send a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname, use the **config client ccx dns-resolve** command.

config client ccx dns-resolve *client_mac_address host_name*

Syntax Description

client_mac_address	MAC address of the client.
host_name	Hostname of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This test does not require the client to use the diagnostic channel.

The following example shows how to send a request to the client 00:E0:77:31:A3:55 to perform the DNS name resolution test to the specified hostname:

```
(Cisco Controller) >config client ccx dns-resolve 00:E0:77:31:A3:55 host_name
```

config client ccx get-client-capability

To send a request to the client to send its capability information, use the **config client ccx get-client-capability** command.

config client ccx get-client-capability *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its capability information:

```
(Cisco Controller) >config client ccx get-client-capability 172.19.28.40
```

config client ccx get-manufacturer-info

To send a request to the client to send the manufacturer's information, use the **config client ccx get-manufacturer-info** command.

config client ccx get-manufacturer-info *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send the manufacturer's information:

```
(Cisco Controller) >config client ccx get-manufacturer-info 172.19.28.40
```

config client ccx get-operating-parameters

To send a request to the client to send its current operating parameters, use the **config client ccx get-operating-parameters** command.

config client ccx get-operating-parameters *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its current operating parameters:

```
(Cisco Controller) >config client ccx get-operating-parameters 172.19.28.40
```

config client ccx get-profiles

To send a request to the client to send its profiles, use the **config client ccx get-profiles** command.

config client ccx get-profiles *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client 172.19.28.40 to send its profile details:

```
(Cisco Controller) >config client ccx get-profiles 172.19.28.40
```

config client ccx log-request

To configure a Cisco client eXtension (CCX) log request for a specified client device, use the **config client ccx log-request** command.

config client ccx log-request {**roam** | **rsna** | **syslog**} *client_mac_address*

Syntax Description

roam	(Optional) Specifies the request to specify the client CCX roaming log.
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.
client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the request to specify the client CCS system log:

```
(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
```

The following example shows how to specify the client CCX roaming log:

```
(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
```

The following example shows how to specify the client CCX RSNA log:

```
(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

To send a message to the client, use the **config client ccx send-message** command.

config client ccx send-message *client_mac_address message_id*

Syntax Description

client_mac_address	MAC address of the client.

message_id

Message type that involves one of the following:

- 1—The SSID is invalid.
- 2—The network settings are invalid.
- 3—There is a WLAN credibility mismatch.
- 4—The user credentials are incorrect.
- 5—Please call support.
- 6—The problem is resolved.
- 7—The problem has not been resolved.
- 8—Please try again later.
- 9—Please correct the indicated problem.
- 10—Troubleshooting is refused by the network.
- 11—Retrieving client reports.
- 12—Retrieving client logs.
- 13—Retrieval complete.
- 14—Beginning association test.
- 15—Beginning DHCP test.
- 16—Beginning network connectivity test.
- 17—Beginning DNS ping test.
- 18—Beginning name resolution test.
- 19—Beginning 802.1X authentication test.
- 20—Redirecting client to a specific profile.
- 21—Test complete.
- 22—Test passed.
- 23—Test failed.
- 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25—Log retrieval refused by the client.
- 26—Client report retrieval refused by the client.
- 27—Test request refused by the client.
- 28—Invalid network (IP) setting.
- 29—There is a known outage or problem with the network.
- 30—Scheduled maintenance period.

(continued on next page)

message_type (cont.)	• 31—The WLAN security method is not correct. • 32—The WLAN encryption method is not correct. • 33—The WLAN authentication method is not correct.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a message to the client MAC address 172.19.28.40 with the message user-action-required:

```
(Cisco Controller) >config client ccx send-message 172.19.28.40 user-action-required
```

config client ccx stats-request

To send a request for statistics, use the **config client ccx stats-request** command.

config client ccx stats-request *measurement_duration* {**dot11** | **security**} *client_mac_address*

Syntax Description

measurement_duration	Measurement duration in seconds.
dot11	(Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify dot11 counter settings:

```
(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

To send a request to the client to terminate the current test, use the **config client ccx test-abort** command.

config client ccx test-abort *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Only one test can be pending at a time.

The following example shows how to send a request to a client to terminate the correct test settings:

```
(Cisco Controller) >config client ccx test-abort 11:11:11:11:11:11
```

config client ccx test-association

To send a request to the client to perform the association test, use the **config client ccx test-association** command.

config client ccx test-association *client_mac_address ssid bssid* **802.11**{**a** | **b** | **g**} *channel*

Syntax Description

client_mac_address	MAC address of the client.
ssid	Network name.
bssid	Basic SSID.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
802.11g	Specifies the 802.11g network.
channel	Channel number.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client MAC address 00:0E:77:31:A3:55 to perform the basic SSID association test:

```
(Cisco Controller) >config client ccx test-association 00:E0:77:31:A3:55 ssid bssid 802.11a
```

config client ccx test-dot1x

To send a request to the client to perform the 802.1x test, use the **config client ccx test-dot1x** command.

config client ccx test-dot1x *client_mac_address profile_id bssid* **802.11** {**a** | **b** | **g**} *channel*

Syntax Description

client_mac_address	MAC address of the client.
profile_id	Test profile name.
bssid	Basic SSID.
802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b network.
802.11g	Specifies the 802.11g network.
channel	Channel number.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client to perform the 802.11b test with the profile name profile_01:

```
(Cisco Controller) >config client ccx test-dot1x 172.19.28.40 profile_01 bssid 802.11b
```

config client ccx test-profile

To send a request to the client to perform the profile redirect test, use the **config client ccx test-profile** command.

config client ccx test-profile *client_mac_address profile_id*

Syntax Description

client_mac_address	MAC address of the client.
profile_id	Test profile name. **Note** The *profile_id* should be from one of the client profiles for which client reporting is enabled.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send a request to the client to perform the profile redirect test with the profile name profile_01:

```
(Cisco Controller) >config client ccx test-profile 11:11:11:11:11:11 profile_01
```

config client deauthenticate

To disconnect a client, use the **config client deauthenticate** command.

config client deauthenticate {*MAC* | *IPv4/v6_address* | *user_name*}

Syntax Description

MAC	Client MAC address.
IPv4/v6_address	IPv4 or IPv6 address.
user_name	Client user name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deauthenticate a client using its MAC address:

```
(Cisco Controller) >config client deauthenticate 11:11:11:11:11
```

config client location-calibration

To configure link aggregation, use the **config client location-calibration** command.

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

Syntax Description

enable	(Optional) Specifies that client location calibration is enabled.
mac_address	MAC address of the client.
interval	Measurement interval in seconds.
disable	(Optional) Specifies that client location calibration is disabled.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the client location calibration for the client 37:15:85:2a with a measurement interval of 45 seconds:

```
(Cisco Controller) >config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

config client profiling delete

To delete client profile , use the **config client profiling** command.

config client profiling delete { *mac_address* }

Syntax Description

mac_address	MAC address of the client.

Command History

Release	Modification
8.2	This command was introduced in this release.

The following example shows how to delete a client profile:

```
(Cisco Controller) >config client profiling delete 37:15:86:2a:Bc:cf
```

Note Executing the above command changes the Device Type to "Unknown". The Client does not get deleted but instead the profiling info of the client is removed, and retains the client as it is still associated. There is no confirmation message from the CLI, due to architecture limitation of the controller.

config cloud-services cmx

To enable or disable CMX Cloud Services, use the **config cloud-services cmx** command.

config cloud-services cmx { **enable** | **disable** }

Syntax Description

enable	Enables the CMX Cloud Services
disable	Disables the CMX Cloud Services

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to enable the CMX Cloud Services:

```
(Cisco Controller) > config cloud-services cmx enable
```

config cloud-services server url

To configure the Cloud Server URL, use the **config cloud-services server url** command.

config cloud-services server url *url*

Syntax Description

url	Enter the Cloud Server URL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure the Cloud Server URL:

```
(Cisco Controller) >config cloud-services server url www.example.com
```

config cloud-services server id-token

To configure the Cloud Server Id-Token, use the **config cloud-services server id-token** command.

config cloud-services server id-token *id-token*

Syntax Description

id-token	Enter the cloud server id-token.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure the Cloud Server Id-Token:

```
(Cisco Controller) >config cloud-services server id-token dzypisQ2#bo$iAQM
```

config coredump

To enable or disable the controller to generate a core dump file following a crash, use the **config cordump** command.

config coredump {**enable** | **disable**}

Syntax Description

enable	Enables the controller to generate a core dump file.
disable	Disables the controller to generate a core dump file.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the controller to generate a core dump file following a crash:

```
(Cisco Controller) > config coredump enable
```

Related Commands

config coredump ftp

config coredump username

show coredump summary

config coredump ftp

To automatically upload a controller core dump file to an FTP server after experiencing a crash, use the **config coredump ftp** command.

config coredump ftp *server_ip_address filename*

Syntax Description

server_ip_address	IP address of the FTP server to which the controller sends its core dump file.
filename	Name given to the controller core dump file.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

The controller must be able to reach the FTP server to use this command.

The following example shows how to configure the controller to upload a core dump file named *core_dump_controller* to an FTP server at network address *192.168.0.13*:

```
(Cisco Controller) > config coredump ftp 192.168.0.13 core_dump_controller
```

Related Commands

config coredump

config coredump username

show coredump summary

config coredump username

To specify the FTP server username and password when uploading a controller core dump file after experiencing a crash, use the **config coredump username** command.

config coredump username *ftp_username* **password** *ftp_password*

Syntax Description

ftp_username	FTP server login username.
ftp_password	FTP server login password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller must be able to reach the FTP server to use this command.

The following example shows how to specify a FTP server username of *admin* and password *adminpassword* for the core dump file upload:

```
(Cisco Controller) > config coredump username admin password adminpassword
```

Related Commands

config coredump ftp

config coredump

show coredump summary

config country

To configure the controller's country code, use the **config country** command.

config country *country_code*

Syntax Description

country_code	Two-letter or three-letter country code.

Command Default

us (country code of the United States of America).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Controllers must be installed by a network administrator or qualified IT professional and the installer must select the proper country code. Following installation, access to the unit should be password-protected by the installer to maintain compliance with regulatory requirements and ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

You can use the **show country** command to display a list of supported countries.

The following example shows how to configure the controller's country code to DE:

```
(Cisco Controller) >config country DE
```

config cts

To enable or disable Cisco TrustSec on controller, use the **config cts** command.

config cts {**enable** | **disable**}

Syntax Description

enable	Enables Cisco TrustSec on the controller
disable	Disables Cisco TrustSec on the controller

Command Default

By default, Cisco TrustSec is in disabled state.

Command History

Release	Modification
8.4	This command was introduced.

config cts ap

To configure inline tagging and security group access control list (SGACL) enforcement on APs, use the **config cts ap** command.

config cts ap {**inline-tagging** | **sgacl-enforcement**} {**enable** | **disable**} {*ap-name* | **all**}

Syntax Description

inline-tagging	Configures inline tagging on all the APs or a specific AP
sgacl-enforcement	Configures SGACL enforcement on all the APs or a specific AP
enable	Enables the specified feature
disable	Disables the specified feature
ap-name	Name of the AP for which the specified feature has to be configured
all	Configures the specified feature for all APs associated with the controller.

Command Default

By default, both inline tagging and SGACL enforcement are in disabled state.

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

- Inline tagging is supported only on the APs in FlexConnect mode.
- Inline tagging is not supported on Flex+Bridge 802.11ac lightweight APs.
- Inline tagging and SGACL download or enforcement are not supported on these controllers: 5508, WiSM2, 8510, 7510, and vWLC.
- If you enable SGACL enforcement for all the APs, the configuration is applied on all the APs except for the APs for which Cisco TrustSec override is enabled.

The following example shows how to enable inline tagging on an AP named *cisco-flex-ap*:

```
(Cisco Controller) >config cts ap inline-tagging enable cisco-flex-ap
```

The following example shows how to enable SGACL enforcement on an AP named *cisco-flex-ap*:

```
(Cisco Controller) >config cts ap sgacl-enforcement enable cisco-flex-ap
```

config cts inline-tag

To configure Cisco TrustSec inline tagging for a controller, use the **config cts inline-tag** command.

config cts inline-tag {**enable** | **disable**}

Syntax Description

inline-tag	Configures inline tagging for the controller
enable	Enables inline tagging
disable	Disables inline tagging

Command Default

By default, inline tagging is in disabled state.

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

Inline tagging is not supported on these controllers: 5508, WiSM2, 8510, 7510, and vWLC.

config cts ap override

To configure Cisco TrustSec override for an AP, use the **config cts ap override** command.

config cts ap override {**enable** | **disable**} {*ap-name*}

Syntax Description

enable	Enables CTS override for the corresponding AP
disable	Disables CTS override for the corresponding AP
ap-name	Name of the AP for which the CTS override has to be configured

Command Default

By default, CTS override for an AP is in disabled state.

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

If you enable SGACL enforcement for all the APs, the configuration is applied on all the APs except the APs for which CTS override is enabled.

The following example shows how to enable CTS override on an AP named *my-cisco-ap*:

```
(Cisco Controller) >config cts ap override enable my-cisco-ap
```

config cts device-id

To configure a Cisco TrustSec device ID, use the **config cts device-id** command.

config cts device-id *device-id* **password** *password*

Syntax Description

device-id	CTS device ID
password	CTS device ID password

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to configure a CTS device ID:

```
(Cisco Controller) > config cts device-id wlc-8540 password Cisco123
```

config cts refresh

To refresh Cisco TrustSec environment data or security group tag (SGT) policy, use the **config cts refresh** command.

config cts refresh {**environment-data**} | {**policy sgt** {**all** | *sgt-tag*}}

Syntax Description

environment-data	Refreshes CTS environment data
policy sgt	Refreshes SGT policy
all	Refreshes all SGT policies
sgt-tag	Enter the CTS SGT tag (an integer) to be refreshed

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

This example shows how to refresh the SGT policy, *Default-65535*:

```
(Cisco Controller) > config cts refresh policy sgt 65535
```

config cts sxp ap connection delete

To delete an SXPv4 connection peer for all the APs or a specific AP, use the **config cts sxp ap connection delete** command.

config cts sxp ap connection delete *ip-addr* {*cisco-ap* | **all**}

Syntax Description

ip-addr	SXPv4 IP address of a peer
cisco-ap	Name of the AP.
all	Applies the configuration to all the APs.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap connection peer

To configure an SXPv4 peer connection for all the APs or a specific AP, use the **config cts sxp ap connection peer** command.

config cts sxp ap connection peer *ip-addr* **password** {**default** | **none**} **mode** {**both** | **listener** | **speaker**} {*cisco-ap* | **all**}

Syntax Description

ip-addr	SXPv4 IP address of the peer
password	Configures password for the SXPv4 peer connection
default	Uses default pasword for MD5 encryption
none	Configures SXPv4 without password encryption
time-in-seconds	Time after which an SXPv4 connection should be tried again after a failure to connect.
mode	Configures mode of the SXPv4 connection
both	Configures device as both SXP speaker and listener
listener	Configures device as SXP listener
speaker	Configures device as SXP speaker
cisco-ap	Name of the AP
all	Applies the configuration to all the APs associated with the corresponding controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

This example shows how to configure an SXPv4 peer connection with a default password and operate in both listener and speaker mode for all the APs associated with the controller:

```
(Cisco Controller) > config cts sxp ap connection peer 10.165.200.224 password default mode
 both all
```

config cts sxp ap default password

To configure the default password for an SXPv4 connection for all the APs or a specific AP, use the **config cts sxp ap default password** command.

config cts sxp ap default password *password* {*cisco-ap* | **all**}

Syntax Description

password	Default password for SXPv4 connection
cisco-ap	Name of the AP
all	Applies the configuration to all the APs associated with the corresponding controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap listener

To configure SXPv4 listener mode parameters, use the **config cts sxp ap listener** command.

config cts sxp ap listener hold-time *min-hold-time max-hold-time* {*cisco-ap* | **all**}

Syntax Description

min-hold-time	Minimum SXPv4 connection hold time
max-hold-time	Maximum SXPv4 connection hold time
cisco-ap	Name of the AP for which SXPv4 has to be configured
all	Configures SXPv4 for all APs associated with the controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap reconciliation period

To configure SXPv4 connection reconciliation time period, use the **config cts sxp ap reconciliation period** command.

config cts sxp ap reconciliation period *time-in-seconds* {*cisco-ap* | **all**}

Syntax Description

time-in-seconds	Time interval until when the SXPv4 connection reconciles. Valid range is between 0 and 64000 seconds.
cisco-ap	Name of the AP
all	Applies the configuration to all the APs associated with the controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap retry period

To configure the interval between SXPv4 connection reattempts, use the **config cts sxp ap retry period** command.

config cts sxp ap retry period *time-in-seconds* {*cisco-ap* | **all**}

Syntax Description

time-in-seconds	Time after which an SXPv4 connection should be attempted again for after a failure to connect. Valid range is between 0 and 64000 seconds.
cisco-ap	Name of the AP
all	Applies the configuration to all the APs associated with the corresponding controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp ap speaker

To configure SXPv4 speaker mode parameters, use the **config cts sxp ap speaker** command.

config cts sxp ap speaker hold-time *time-in-seconds* {*cisco-ap* | **all**}

Syntax Description

time-in-seconds	Hold time interval, in seconds. Valid range is between 1 and 65534 seconds.
cisco-ap	Name of the AP for which SXPv4 has to be configured
all	Configures SXPv4 for all APs associated with the corresponding controller

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp

To enable or disable Cisco TrustSec SXP on a controller, use the **config cts sxp** command.

config cts sxp {**enable** | **disable**}

Syntax Description

enable	Enables Cisco TrustSec SXP on the controller
disable	Disables Cisco TrustSec SXP on the controller

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp connection

To configure the CTS SXP connection on the controller, use the **config cts sxp connection** command.

config cts sxp connection {**delete** | **peer**} *ipv4-addr*

Syntax Description

delete	Deletes the SXP connection
peer	Configures the next hop switch with which the controller is connected
ipv4-addr	IPv4 address of the SXP connection

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp default password

To configure the default password for CTS SXP, use the **config cts sxp default password** command.

config cts sxp default password *password*

Syntax Description

password	Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp retry period

To configure the interval between CTS SXP connection reattempts, use the **config cts sxp retry period** command.

config cts sxp retry period *time-in-seconds*

Syntax Description

time-in-seconds	Time after which a CTS SXP connection should be attempted again for after a failure to connect. Valid range is between 0 and 64000 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

config cts sxp version

To configure the CTS SXP connection version, use the **config cts sxp version** command.

config cts sxp version *version-1-or-2*

Syntax Description

version-1-or-2	Enter the SXP version. Valid values are 1 and 2

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

config cts sxp

To configure Cisco TrustSec SXP (CTS) connections on the controller, use the **config cts sxp** command.

config cts sxp {**enable** | **disable** | **connection** {**delete** | **peer**} | **default password** *password* | **retry period** *time-in-seconds*}

Syntax Description

enable	Enables CTS connections on the controller.
disable	Disables CTS connections on the controller.
connection	Configures CTS connection on the controller.
delete	Deletes the CTS connection on the controller.
peer	Configures the next hop switch with which the controller is connected.
ip-address	Only IPv4 address of the peer.
default password	Configures the default password for MD5 authentication of SXP messages.
password	Default password for MD5 Authentication of SXP messages. The password should contain a minimum of six characters.
retry period	Configures the SXP retry period.
time-in-seconds	Time after which a CTS connection should be again tried for after a failure to connect.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For release 8.0, only IPv4 is supported for TrustSec SXP configuration.

The following example shows how to enable CTS on the controller:

```
(Cisco Controller) > config cts sxp enable
```

The following example shows how to configure a peer for a CTS connection:

```
> config cts sxp connection peer 209.165.200.224
```

Related Commands

debug cts sxp

config custom-web ext-webauth-mode

To configure external URL web-based client authorization for the custom-web authentication page, use the **config custom-web ext-webauth-mode** command.

config custom-web ext-webauth-mode {**enable** | **disable**}

Syntax Description

enable	Enables the external URL web-based client authorization.
disable	Disables the external URL we-based client authentication.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the external URL web-based client authorization:

```
(Cisco Controller) > config custom-web ext-webauth-mode enable
```

Related Commands

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

To configure the complete external web authentication URL for the custom-web authentication page, use the **config custom-web ext-webauth-url** command.

config custom-web ext-webauth-url *URL*

Syntax Description

URL	URL used for web-based client authorization.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the complete external web authentication URL http://www.AuthorizationURL.com/ for the web-based client authorization:

```
(Cisco Controller) > config custom-web ext-webauth-url http://www.AuthorizationURL.com/
```

Related Commands

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

To configure an external web server, use the **config custom-web ext-webserver** command.

config custom-web ext-webserver {**add** *index IP_address* | **delete** *index*}

Syntax Description

add	Adds an external web server.
index	Index of the external web server in the list of external web server. The index must be a number between 1 and 20.
IP_address	IP address of the external web server.
delete	Deletes an external web server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to add the index of the external web server 2 to the IP address of the external web server 192.23.32.19:

```
(Cisco Controller) > config custom-web ext-webserver add 2 192.23.32.19
```

Related Commands

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

To enable or disable the custom web authentication logout popup, use the **config custom-web logout-popup** command.

config custom-web logout-popup {**enable** | **disable**}

Syntax Description

enable	Enables the custom web authentication logout popup. This page appears after a successful login or a redirect of the custom web authentication page.
disable	Disables the custom web authentication logout popup.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the custom web authentication logout popup:

```
(Cisco Controller) > config custom-web logout-popup disable
```

Related Commands

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 qrscan-bypass-opt

To configure the qrscan bypass authentication options, use the **config custom-web qrscan-bypass-opt** command.

config custom-web qrscan-bypass-opt *timer count*

Syntax Description

timer	Set the duration to bypass the traffic temporarily. The range is between 5 and 60.
count	Set the number of times the traffic can be bypassed before client rejoins. The range is between 1 and 9.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to set the custom qrscan bypass timer to 60 and number of times to 3 before the client rejoins:

```
(Cisco Controller) > config custom-web qrscan-bypass-opt 60 3
```

config custom-web radiusauth

To configure the RADIUS web authentication method, use the **config custom-web radiusauth** command.

config custom-web radiusauth {**chap** | **md5chap** | **pap**}

Syntax Description

chap	Configures the RADIUS web authentication method as Challenge Handshake Authentication Protocol (CHAP).
md5chap	Configures the RADIUS web authentication method as Message Digest 5 CHAP (MD5-CHAP).
pap	Configures the RADIUS web authentication method as Password Authentication Protocol (PAP).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the RADIUS web authentication method as MD5-CHAP:

```
(Cisco Controller) > config custom-web radiusauth md5chap
```

Related Commands

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

To configure the redirect URL for the custom-web authentication page, use the **config custom-web redirectUrl** command.

config custom-web redirectUrl *URL*

Syntax Description

URL	URL that is redirected to the specified address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the URL that is redirected to abc.com:

```
(Cisco Controller) > config custom-web redirectUrl abc.com
```

Related Commands

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

To delete a web-authenticated sleeping client, use the **config custom-web sleep-client** command.

config custom-web sleep-client delete *mac_address*

Syntax Description

delete	Deletes a web-authenticated sleeping client with the help of the client MAC address.
mac_address	MAC address of the sleeping client.

Command Default

The web-authenticated sleeping client is not deleted.

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to delete a web-authenticated sleeping client:

```
(Cisco Controller) > config custom-web sleep-client delete 0:18:74:c7:c0:90
```

config custom-web webauth-type

To configure the type of web authentication, use the **config custom-web webauth-type** command.

config custom-web webauth-type {**internal** | **customized** | **external**}

Syntax Description

internal	Configures the web authentication type to internal.
customized	Configures the web authentication type to customized.
external	Configures the web authentication type to external.

Command Default

The default web authentication type is **internal**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the type of the web authentication type to internal:

```
(Cisco Controller) > config custom-web webauth-type internal
```

Related Commands

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

To configure the web authentication logo for the custom-web authentication page, use the **config custom-web weblogo** command.

config custom-web weblogo {**enable** | **disable**}

Syntax Description

enable	Enables the web authentication logo settings.
disable	Enable or disable the web authentication logo settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the web authentication logo:

```
(Cisco Controller) > config custom-web weblogo enable
```

Related Commands

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

To configure the custom web authentication message text for the custom-web authentication page, use the **config custom-web webmessage** command.

config custom-web webmessage *message*

Syntax Description

message	Message text for web authentication.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the message text Thisistheplace for webauthentication:

```
(Cisco Controller) > config custom-web webmessage Thisistheplace
```

Related Commands

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

To configure the web authentication title text for the custom-web authentication page, use the **config custom-web webtitle** command.

config custom-web webtitle *title*

Syntax Description

title	Custom title text for web authentication.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the custom title text Helpdesk for web authentication:

```
(Cisco Controller) > config custom-web webtitle Helpdesk
```

Related Commands

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

To configure the local database, use the **config database size** command.

config database size *count*

Syntax Description		
	count	Database size value between 512 and 2040

Command Default None

Command History	Release	Modification
	7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines Use the **show database** command to display local database configuration.

The following example shows how to configure the size of the local database:

```
(Cisco Controller) > config database size 1024
```

Related Commands **show database**

config dhcp

To configure the internal DHCP, use the **config dhcp** command.

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* }

Syntax Description

address-pool *scope start end*	Configures an address range specify the scope name and addresses of the address rang
create-scope *name*	Creates a new DHCP scope. scope name.
default-router *scope router_1* [*router_2*] [*router_3*]	Configures the default routers and specify the IP address o you can specify the IP addre tertiary routers.
delete-scope *scope*	Deletes the specified DHCP
disable *scope*	Disables the specified DHCI
dns-servers *scope dns1* [*dns2*] [*dns3*]	Configures the name servers You must also specify at lea Optionally, you can specify name servers.
domain *scope domain*	Configures the DNS domain specify the scope and domai
enable *scope*	Enables the specified dhcp s
lease *scope lease_duration*	Configures the lease duratio specified scope.
netbios-name-server *scope wins1* [*wins2*] [*wins3*]	Configures the netbios name specify the scope name and t server. Optionally, you can s of secondary and tertiary na
network *scope network netmask*	Configures the network and specify the scope name, the the network mask.

opt-82 remote-id	Configures the DHCP option 82 format. DHCP option 82 provides additi DHCP is used to allocate netwo controller acts as a DHCP relay DHCP client requests from untr controller adds option 82 inform requests from clients before forw to the DHCP server.
ap_mac	MAC address of the access poin option 82 payload.
*ap_mac***:***ssid*	MAC address and SSID of the a DHCP option 82 payload.
ap-ethmac	Remote ID format as AP Ethern
apname:ssid	Remote ID format as AP name:
ap-group-name	Remote ID format as AP group
flex-group-name	Remote ID format as FlexConn
ap-location	Remote ID format as AP locatio
apmac-vlan_id	Remote ID format as AP radio M address:VLAN_ID.
apname-vlan_id	Remote ID format as AP Name:
ap-ethmac-ssid	Remote ID format as AP Ethern address.

Command Default

The default value for ap-group-name is default-group, and for ap-location, the default value is default location.

If ap-group-name and flex-group-name are null, the system MAC is sent as the remote ID field.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **show dhcp** command to display the internal DHCP configuration.

The following example shows how to configure the DHCP lease for the scope 003:

```
(Cisco Controller) >config dhcp lease 003
```

config dhcp opt-82 format

To configure the DHCP option 82 format, use the **config dhcp opt-82 format** command.

config dhcp opt-82 format {*binary* | *ascii*}

Syntax Description

binary	Specifies the DHCP option 82 format as binary.
ascii	Specifies the DHCP option 82 format as ASCII.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the format of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 format binary
```

config dhcp opt-82 remote-id

To configure the format of the DHCP option 82 payload, use the **config dhcp opt-82 remote-id** command.

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*}

Syntax Description

ap_mac	Specifies the radio MAC address of the access point to the DHCP option 82 payload.
ap_mac:ssid	Specifies the radio MAC address and SSID of the access point to the DHCP option 82 payload.
ap-ethmac	Specifies the Ethernet MAC address of the access point to the DHCP option 82 payload.
apname:ssid	Specifies the AP name and SSID of the access point to the DHCP option 82 payload.
ap-group-name	Specifies the AP group name to the DHCP option 82 payload.
flex-group-name	Specifies the FlexConnect group name to the DHCP option 82 payload.
ap-location	Specifies the AP location to the DHCP option 82 payload.
apmac-vlan-id	Specifies the radio MAC address of the access point and the VLAN ID to the DHCP option 82 payload.
apname-vlan-id	Specifies the AP name and its VLAN ID to the DHCP option 82 payload.
ap-ethmac-ssid	Specifies the Ethernet MAC address of the access point and the SSID to the DHCP option 82 payload.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the remote ID of DHCP option 82 payload:

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

config dhcp proxy

To specify the level at which DHCP packets are modified, use the **config dhcp proxy** command.

config dhcp proxy {**enable** | **disable** {**bootp-broadcast** [**enable** | **disable**]}

Syntax Description

enable	Allows the controller to modify the DHCP packets without a limit.
disable	Reduces the DHCP packet modification to the level of a relay.
bootp-broadcast	Configures DHCP BootP broadcast option.

Command Default

DHCP is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **show dhcp proxy** command to display the status of DHCP proxy handling.

To enable third-party WGB support, you must enable the passive-client feature on the wirless LAN by entering the **config wlan passive-client enable** command.

The following example shows how to disable the DHCP packet modification:

```
(Cisco Controller) >config dhcp proxy disable
```

The following example shows how to enable the DHCP BootP broadcast option:

```
(Cisco Controller) >config dhcp proxy disable bootp-broadcast enable
```

config dhcp timeout

To configure a DHCP timeout value, use the **config dhcp timeout** command. If you have configured a WLAN to be in DHCP required state, this timer controls how long the controller will wait for a client to get a DHCP lease through DHCP.

config dhcp timeout *timeout-value*

Syntax Description

timeout-value	Timeout value in the range of 5 to 120 seconds.

Command Default

The default timeout value is 120 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the DHCP timeout to 10 seconds:

```
(Cisco Controller) >config dhcp timeout 10
```

config dx

To configure data externalization on a controller, use the **config dx** command.

config dx {**enable** | **disable**}

Syntax Description

enable	Enables data externalization on controller.
disable	Disables data externalization on controller.

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

If you have enabled data externalization on Cisco 5508 WLC, the maximum number of APs that the WLC can support is capped at 250.

config exclusionlist

To create or delete an exclusion list entry, use the **config exclusionlist** command.

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*]}

Syntax Description

config exclusionlist	Configures the exclusion list.
add	Creates a local exclusion-list entry.
delete	Deletes a local exclusion-list entry
description	Specifies the description for an exclusion-list entry.
MAC	MAC address of the local Excluded entry.
description	(Optional) Description, up to 32 characters, for an excluded entry.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

The following example shows how to delete a local exclusion list entry for the MAC address *xx:xx:xx:xx:xx:xx:*

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

Related Commands

show exclusionlist

config fabric

To enable or disable fabric, use the **config fabric** command.

config fabric enable disable

Syntax Description

enable	Enables fabric.
disable	Disables fabric.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Example

The following example shows how to enable fabric:

```
config fabric enable
```

config fabric vnid create name

To configure the fabric Virtual Extensible LAN (VXLAN) network identifier (VNID) and subnet, use the **config fabric vnid create name** command.

config fabric vnid create name *interface-name* **l2-vnid** *l2-vnid* **ip** *network-ip* **subnet** *subnet* **l3-vnid** *l3-vnid*

Syntax Description

interface-name	Name of the interface.
l2-vnid	Layer 2 VNID.
L2-vnid	Layer 2 VNID value.
ip	IP address.
network-ip	Network IP address.
subnet	Subnet address.
subnet	Subnet address of the network.
L3-vnid	Layer 3 VNID value.
l3-vnid	Layer 3 VNID.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The Subnet to VNID combination is expected to 1:1 with no-overlaps.

The VNID name can be used for Radius override or configuration of VNID on WLAN.

The guest fabric VNID or subnet should not overlap with the enterprise fabric VNID or subnet.

Examples

The following example shows how to configure fabric VNID and its subnet:

```
(Cisco Controller) >config fabric vnid create name vnid1 l2-vnid l2-vn ip 10.10.1.3 subnet
 255.255.255.223 l3-vnid l3-vn
```

config fabric control-plane enterprise-fabric

To configure IP address of the mapserver and the pre-shared key, use the **config fabric control-plane enterprise-fabric ip** command.

config fabric control-plane enterprise-fabric {add |delete}{primary | secondary} ip *ip-address* **preshared-key** *pre-shared-key*

Syntax Description

ip-address	IP address of the mapserver.
pre-shared-key	Pre-shared key.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The AP should be part of the fabric on the mapserver configured using this command. You can use a maximum of 2 IP addresses, which will be in active-active mode .

Use **config fabric control-plane enterprise-fabric delete ip***ip-address*command to delete the associated map server.

Examples

The following example shows how to configure IP address of the mapserver and the pre-shared key:

```
(Cisco Controller) >config fabric control-plane enterprise-fabric add primary ip 10.1.1.1
preshare-key secret
```

config fabric control-plane guest-fabric

To configure IP address of the guest mapserver and the pre-shared key used for the fabric WLAN, use the **config fabric control-plane guest-fabric** command.

config fabric control-plane guest-fabric {add |delete}{primary | secondary} ip *ip-address* **preshared-key** *pre-shared-key*

Syntax Description

ip-address	IP address of the mapserver.
pre-shared-key	Pre-shared key.

Command Default

Enterprise fabic mapserver is used.

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

You can use a maximum of 2 IP addresses, which will be in active-active mode .

Examples

The following example shows how to configure IP address of the guest mapserver and the pre-shared key:

```
(Cisco Controller) >config fabric control-plane guest-fabric add primary ip 10.2.1.1
preshared-key guest
```

config flexconnect [ipv6] acl

To apply access control lists that are configured on a FlexConnect access point, use the **config flexconnect** [**ipv6**] **acl** command. Use the **ipv6** keyword to configure IPv6 FlexConnect ACLs .

config flexconnect [**ipv6**] **acl** {**apply** | **create** | **delete**} *acl_name*

Syntax Description

ipv6	Use this option to configure IPv6 FlexConnect ACLs. If you don't use this option, then IPv4 FlexConnect ACLs will be configured.
apply	Applies an ACL to the data path.
create	Creates an ACL.
delete	Deletes an ACL.
acl_name	ACL name that contains up to 32 alphanumeric characters.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.8	IPv6 ACL option was introduced.

The following example shows how to apply the IPv4 ACL configured on a FlexConnect access point:

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect [ipv6] acl rule

To configure access control list (ACL) rules on a FlexConnect access point, use the **config flexconnect** [**ipv6**] **acl rule** command.

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*}

Syntax Description

ipv6	Use this option to configure IPv6 FlexConnect ACL rules. If you don't use this option, then IPv4 FlexConnect ACL rules will be configured.
action	Configures whether to permit or deny access.
rule_name	ACL name that contains up to 32 alphanumeric characters.
rule_index	Rule index between 1 and 32.
permit	Permits the rule action.
deny	Denies the rule action.
add	Adds a new rule.
change	Changes a rule's index.
index	Specifies a rule index.
delete	Deletes a rule.
destination address	Configures a rule's destination IP address and netmask.
ip_address	IP address of the rule.
netmask	Netmask of the rule.
start_port	Start port number (between 0 and 65535).
end_port	End port number (between 0 and 65535).
direction	Configures a rule's direction to in, out, or any.
in	Configures a rule's direction to in.
out	Configures a rule's direction to out.
any	Configures a rule's direction to any.
dscp	Configures a rule's DSCP.

dscp	Number between 0 and 63, or **any**.
protocol	Configures a rule's DSCP.
protocol	Number between 0 and 255, or **any**.
source address	Configures a rule's source IP address and netmask.
source port range	Configures a rule's source port range.
swap	Swaps two rules' indices.
index_1	The rule first index to swap.
index_2	The rule index to swap the first index with.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.8	IPv6 ACL option was introduced.

This example shows how to configure an ACL to permit access:

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect [ipv6] acl url-domain

To configure a URL domain-based rule for a FlexConnect ACL, use the **config flexconnect acl** [**ipv6**] **url-domain** command.

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*}

Syntax Description

ipv6	Use this option to configure URL domain-based rules for IPv6 FlexConnect ACLs. If you don't use this option, then IPv4 FlexConnect ACL rules will be configured.
action *acl-name index action*	Configures the action for the FlexConnect ACL rule, whether to permit or deny access.
add *acl-name index*	Adds URL domain to the FlexConnect ACL.
delete *acl-name index*	Deletes the URL domain from the FlexConnect ACL.
url *acl-name index url-name*	Configures the URL name in the FlexConnect ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.8	IPv6 ACL option was introduced.

This example shows how to configure URL-based rule for an IPv6 FlexConnect ACL:

```
(Cisco Controller) >config flexconnect ipv6 acl url-domain action acls-to-allow 2 permit
```

config flexconnect arp-caching

To save an ARP entry for a client in the cache with locally switched WLAN on FlexConnect APs or in a software-defined access (Fabric) deployment, use **config flexconnect arp-caching** command.

config flexconnect arp-caching {**enable** } **disable**}

Syntax Description

arp-caching enable	Instructs the access point to save the ARP entry for a client in the cache and reply on its behalf of the client for locally switched WLAN.
arp-caching disable	Disables ARP caching.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.
8.5.151.0, 8.8.12x.0, 8.9.111.0, 8.10	This command was made applicable to software-defined access deployments as well.

Example

The following example shows how to apply the proxy ARP with locally switched WLAN on FlexConnect APs.

```
(Cisco Controller) >config flexconnect arp-caching enable
```

config flexconnect avc profile

To configure a Flexconnect Application Visibility and Control (AVC) profile, use the **config flexconnect avc profile** command.

config flexconnect avc profile *profilename* {**create | delete**} | **apply** | **rule** {**addapplication** *app-name* {**drop** | {**mark** *dscp-value*}}} | {**remove application** *app-name*}

Syntax Description

proflie-name	Name of the AVC profile. The range is from 0 to 32 alphanumeric characters.
create	Creates an AVC profile.
delete	Deletes an AVC profile.
apply	Applies an AVC profile.
rule	Configures a Rule for an AVC profile.
add application	Adds a rule for an AVC profile.
app-name	Name of the application. The range is from 0 to 32 alphanumeric characters.
drop	Adds a rule to drop packets.
mark	Adds a rule to mark packets with specific differentiated services code point (DSCP).
dscp-value	DSCP value for marking packets. The range is from 0 to 63.
remove application	Removes a rule for an AVC profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create a FlexConnect profile:

```
(Cisco Controller) >config flexconnect avc profile profile1 create
```

config flexconnect fallback-radio-shut

To configure the radio interface of an access point when the Ethernet link is not operational, use the **config flexconnect fallback-radio-shut** command.

config flexconnect fallback-radio-shut {**disable** | **enable delay** *delay-in-sec*}

Syntax Description

disable	Disables the radio interface shutdown.
enable	Enables the radio interface shutdown.
delay	Specifies the delay for the interface after which the radio interface has to be shut down.
delay-in-sec	Delay duration, in seconds.

Command Default

The radio interface shutdown is disabled.

Command History

Release	Modification
7.6	This command was introduced.

Usage Guidelines

You can specify the delay duration only if you enable the radio interface shutdown.

The following example shows how to enable the radio interface shutdown after a delay duration of 5 seconds:

```
(Cisco Controller) >config flexconnect fallback-radio-shut enable delay 5
```

config flexconnect group

To add, delete, or configure a FlexConnect group, use the **config flexconnect group** command.

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*

Syntax Description

group_name	Group name.
add	Adds a FlexConnect group.
delete	Deletes a FlexConnect group.
ap	Adds or deletes an access poin
add	Adds an access point to a Flex
delete	Deletes an access point to a Fl
ap_mac	MAC address of the access po
radius	Configures the RADIUS serve FlexConnect group.
ap	Configures an access point bas authentication for a FlexConn
authority	Configures the Extensible Aut Authentication via Secure Tun parameters.
id	Configures the authority ident
hex_id	Authority identifier of the loca characters. You can enter up to characters.
info	Configures the authority ident text format.

auth_info	Authority identifier of the
disable	Disables an AP based RAI
eap-fast	Enables or disables Extens Authentication via Secure
enable	Enables EAP-FAST auther
disable	Disables EAP-FAST authe
enable	Enables AP based RADIU
leap	Enables or disables Lightw (LEAP) authentication.
disable	Disables LEAP authentica
enable	Enables LEAP authenticat
pac-timeout	Configures the EAP-FAST parameters.
timeout	PAC timeout in days. The indicates that it is disabled
server-key	Configures the EAP-FAST encrypt and decrypt PACs.
auto	Automatically generates a
key	Key that disables efficient
user	Manages the user list at the
add	Adds a user. You can confi
username	Username that is case-sens 24 characters.
password	Password of the user.
delete	Deletes a user.
server	Configures an external RA
add	Adds an external RADIUS
delete	Deletes an external RADIU
primary	Configures an external pri
secondary	Configures an external sec
IP_address	IP address of the RADIUS

auth_port	Port address of the RADIUS s
secret	Index of the RADIUS server.
predownload	Configures an efficient AP upg can download an upgrade imag without resetting the access po
disable	Disables an efficient upgrade f
enable	Enables an efficient upgrade fe
master	Manually designates an access primary AP.
ap_name	Access point name.
slave	Manually designates an access subordinate AP.
retry-count	Configures the number of time predownload an image from th
max_count	Maximum number of times the predownload an image from th
ap_name	Override the manually configu
cisco_ap	Name of the primary access po
start	Starts the predownload image
primary	Starts the predownload primar group.
backup	Starts the predownload backup group.
abort	Terminates the predownload in group.
local-split	Configures a local-split ACL o
wlan	Configures a WLAN for a local
wlan_id	Wireless LAN identifier betwe
acl	Configures a local split ACL on
acl_name	Name of the ACL.
multicast overridden-interface	Configures multicast across th overridden interface for locally
vlan	Configures a VLAN to the Fle

add	Adds a VLAN to the FlexC
vlan_id	VLAN identifier.
in-acl	Inbound ACL name that co
out-acl	Outbound ACL name that c
delete	Deletes a VLAN from the
web-auth	Configures a FlexConnect
wlan	Specifies the wireless LAN
wlan_id	Wireless LAN identifier be
cisco_ap	Name of the FlexConnect a
acl	Configures a FlexConnect
web-policy	Configures a web policy F
add	Adds a web policy FlexCo
delete	Deletes a web policy FlexC
eap-cert download	Downloads the EAP root a
eap-tls	Enables or disables EAP-T authentication.
peap	Enables or disables Protect (PEAP) authentication.
policy acl	Configures policy ACL on
http-proxy ipaddress	Configures http-proxy serv

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can add up to 100 clients.

Beginning in Release 7.4 and later releases, the supported maximum number of RADIUS servers is 100.

The following example shows how to add a FlexConnect group for MAC address 192.12.1.2:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 add
```

The following example shows how to add a RADIUS server as a primary server for a FlexConnect group with the server index number 1:

```
(Cisco Controller) >config flexconnect group 192.12.1.2 radius server add primary 1
```

The following example shows how to enable a local split ACL on a FlexConnect AP group for a WLAN:

```
(Cisco Controller) >config flexconnect group flexgroup1 local-split wlan 1 acl flexacl1
enable
```

config flexconnect group vlan

To configure VLAN for a FlexConnect group, use the **config flexconnect group vlan** command.

config flexconnect group *group_name* **vlan** {**add** *vlan-id* **acl** *in-aclname out-aclname* | **delete** *vlan-id*}

Syntax Description

group_name	FlexConnect group name.
add	Adds a VLAN for the FlexConnect group.
vlan-id	VLAN ID.
acl	Specifies an access control list.
in-aclname	In-bound ACL name.
out-aclname	Out-bound ACL name.
delete	Deletes a VLAN from the FlexConnect group.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add VLAN ID 1 for the FlexConnect group myflexacl where the in-bound ACL name is in-acl and the out-bound ACL is out-acl:

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

config flexconnect group *group-name* dhcp overridden-interface

To enable or disable the DHCP overridden interface for a FlexConnect group, use the **config flexconnect group** *group-name* **dhcp overridden-interface** command.

config flexconnect group *group-name* **dhcp overridden-interface** {**enable** | **disable**}

Syntax Description

overridden-interface	The DHCP overridden interface for FlexConnect group.
group-name	Name of the FlexConnect group.
enable	Instructs the access point to enable DHCP broadcast for locally switched clients.
disable	Disables the feature.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example shows how to enable DHCP broadcast for locally switched clients.

```
(Cisco Controller) >config flexconnect
  group flexgroup dhcp overridden-interface enable
```

config flexconnect group web-auth

To configure Web-Auth ACL for a FlexConnect group, use the **config flexconnect group web-auth** command.

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

Syntax Description

group_name	FlexConnect group name.
wlan-id	WLAN ID.
acl-name	ACL name.
enable	Enables the Web-Auth ACL for a FlexConnect group.
disable	Disables the Web-Auth ACL for a FlexConnect group.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable Web-Auth ACL webauthacl for the FlexConnect group myflexacl on WLAN ID 1:

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl enable
```

config flexconnect group web-policy

To configure Web Policy ACL for a FlexConnect group, use the **config flexconnect group web-policy** command.

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

Syntax Description

group_name	FlexConnect group name.
add	Adds the Web Policy ACL.
delete	Deletes the Web Policy ACL.
acl-name	Name of the Web Policy ACL.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add the Web Policy ACL mywebpolicyacl to the FlexConnect group myflexacl:

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

config flexconnect join min-latency

To enable or disable the access point to choose the controller with the least latency when joining, use the **config flexconnect join min-latency** command.

config flexconnect join min-latency {**enable** | **disable**} *cisco_ap*

Syntax Description

enable	Enables the access point to choose the controller with the least latency when joining.
disable	Disables the access point to choose the controller with the least latency when joining.
cisco_ap	Cisco lightweight access point.

Command Default

The access point cannot choose the controller with the least latency when joining.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable this feature, the access point calculates the time between the discovery request and discovery response and joins the controller that responds first. This command is supported only on the following controller releases:

- Cisco 2500 Series Controller
- Cisco 5500 Series Controller
- Cisco Flex 7500 Series Controllers
- Cisco 8500 Series Controllers
- Cisco Wireless Services Module 2

This configuration overrides the HA setting on the controller, and is applicable only for OEAP access points.

The following example shows how to enable the access point to choose the controller with the least latency when joining:

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

config flexconnect office-extend

To configure FlexConnect mode for an OfficeExtend access point, use the **config flexconnect office-extend** command.

config flexconnect office-extend {{**enable** | **disable**} *cisco_ap* | **clear-personalssid-config** *cisco_ap*}

Syntax Description

enable	Enables the OfficeExtend mode for an access point.
disable	Disables the OfficeExtend mode for an access point.
clear-personalssid-config	Clears only the access point's personal SSID.
cisco_ap	Cisco lightweight access point.

Command Default

OfficeExtend mode is enabled automatically when you enable FlexConnect mode on the access point.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Currently, only Cisco Aironet 1130 series and 1140 series access points that are joined to a Cisco 5500 Series Controller with a WPlus license can be configured to operate as OfficeExtend access points.

Rogue detection is disabled automatically when you enable the OfficeExtend mode for an access point. OfficeExtend access points, which are deployed in a home environment, are likely to detect a large number of rogue devices. You can enable or disable rogue detection for a specific access point or for all access points by using the **config rogue detection** command.

DTLS data encryption is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable DTLS data encryption for a specific access point or for all access points by using the **config ap link-encryption** command.

Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable Telnet or SSH access for a specific access point by using the **config ap telnet** or **config ap ssh** command.

Link latency is enabled automatically when you enable the OfficeExtend mode for an access point. However, you can enable or disable link latency for a specific access point or for all access points currently associated to the controller by using the **config ap link-latency** command.

The following example shows how to enable the office-extend mode for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend enable Cisco_ap
```

The following example shows how to clear only the access point's personal SSID for the access point Cisco_ap:

```
(Cisco Controller) >config flexconnect office-extend clear-personalssid-config Cisco_ap
```

config flow

To configure a NetFlow Monitor and Exporter, use the **config flow** command.

config flow {**add** | **delete**} **monitor** *monitor_name* {**exporter** *exporter_name* | **record**{*ipv4_client_app_flow_record* | *ipv4_client_src_dst_flow_record*}

Syntax Description

add	Associates either a NetFlow monitor with an exporter, or a NetFlow record with a NetFlow monitor.
delete	Dissociates either a NetFlow monitor from an exporter, or a NetFlow record from a NetFlow monitor.
monitor	Configures a NetFlow monitor.
monitor_name	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces in a monitor name.
exporter	Configures a NetFlow exporter.
exporter_name	Name of the NetFlow exporter. The exporter name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces in an exporter name.
record	Associates a NetFlow record to the NetFlow monitor.
ipv4_client_app_flow_record	Existing record template for better performance.
ipv4_client_src_dst_flow_record	Enhanced record template for better coverage.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

An exporter is a network entity that exports the template with IP traffic information. The controller acts as an exporter. A NetFlow record in the controller contains the information about the traffic in a given flow, such as client MAC address, client source IP address, WLAN ID, incoming and outgoing bytes of data, incoming and outgoing packets, and incoming and outgoing Differentiated Services Code Point (DSCP).

The following example shows how to configure a NetFlow monitor and exporter:

```
(Cisco Controller) > config flow add monitor monitor1 exporter exporter1
```

config guest-lan

To create, delete, enable or disable a wireless LAN, use the **config guest-lan** command.

config guest-lan {**create** | **delete**} *guest_lan_id interface_name* | {**enable** | **disable**} *guest_lan_id*

Syntax Description

create	Creates a wired LAN settings.
delete	Deletes a wired LAN settings:
guest_lan_id	LAN identifier between 1 and 5 (inclusive).
interface_name	Interface name up to 32 alphanumeric characters.
enable	Enables a wireless LAN.
disable	Disables a wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan enable 16
```

Related Commands

show wlan

config guest-lan custom-web ext-webauth-url

To redirect guest users to an external server before accessing the web login page, use the **config guest-lan custom-web ext-webauth-url** command.

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

Syntax Description

ext_web_url	URL for the external server.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a wireless LAN with the LAN ID 16:

```
(Cisco Controller) > config guest-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web login_page

config guest-lan custom-web global disable

To use a guest-LAN specific custom web configuration rather than a global custom web configuration, use the **config guest-lan custom-web global disable** command.

config guest-lan custom-web global disable *guest_lan_id*

Syntax Description

guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you enter the **config guest-lan custom-web global enable** *guest_lan_id* command, the custom web authentication configuration at the global level is used.

The following example shows how to disable the global web configuration for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web global disable 1
```

Related Commands

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

To enable wired guest users to log into a customized web login page, use the **config guest-lan custom-web login_page** command.

config guest-lan custom-web login_page *page_name guest_lan_id*

Syntax Description

page_name	Name of the customized web login page.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to customize a web login page custompage1 for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web login_page custompage1 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web webauth-type

To define the web login page for wired guest users, use the **config guest-lan custom-web webauth-type** command.

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

Syntax Description

internal	Displays the default web login page for the controller. This is the default value.
customized	Displays the custom web login page that was previously configured.
external	Redirects users to the URL that was previously configured.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

The default web login page for the controller is internal.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the guest LAN with the webauth-type as internal for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan custom-web webauth-type internal 1
```

Related Commands

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan ingress-interface

To configure the wired guest VLAN's ingress interface that provides a path between the wired guest client and the controller through the Layer 2 access switch, use the **config guest-lan ingress-interface** command.

config guest-lan ingress-interface *guest_lan_id interface_name*

Syntax Description

guest_lan_id	Guest LAN identifier from 1 to 5 (inclusive).
interface_name	Interface name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to provide a path between the wired guest client and the controller with guest LAN ID 1 and the interface name guest01:

```
(Cisco Controller) > config guest-lan ingress-interface 1 guest01
```

Related Commands

config interface guest-lan

config guest-lan create

config guest-lan interface

To configure an egress interface to transmit wired guest traffic out of the controller, use the **config guest-lan interface** command.

config guest-lan interface *guest_lan_id interface_name*

Syntax Description

guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).
interface_name	Interface name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an egress interface to transmit guest traffic out of the controller for guest LAN ID 1 and interface name guest01:

```
(Cisco Controller) > config guest-lan interface 1 guest01
```

Related Commands

config ingress-interface guest-lan

config guest-lan create

config guest-lan mobility anchor

To add or delete mobility anchor, use the **config guest-lan mobility anchor** command.

config guest-lan mobility anchor {**add** | **delete**} *Guest LAN Id IP addr*

Syntax Description

add	Adds a mobility anchor to a WLAN.
delete	Deletes a mobility anchor from a WLAN.
Guest LAN Id	Guest LAN identifier between 1 and 5.
IP addr	Member switch IPv4 or IPv6 address to anchor WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to delete a mobility anchor for WAN ID 4 and the anchor IP *192.168.0.14*:

```
(Cisco Controller) > config guest-lan mobility anchor delete 4 192.168.0.14
```

config guest-lan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a guest LAN, use the **config guest-lan nac** command:

config guest-lan nac {**enable** | **disable**} *guest_lan_id*

Syntax Description

enable	Enables the NAC out-of-band support.
disable	Disables the NAC out-of-band support.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the NAC out-of-band support for guest LAN ID 3:

```
(Cisco Controller) > config guest-lan nac enable 3
```

Related Commands

show nac statistics

show nac summary

config wlan nac

debug nac

config guest-lan security

To configure the security policy for the wired guest LAN, use the **config guest-lan security** command.

config guest-lan security {**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *guest_lan_id* | **web-passthrough** {**acl** | **email-input** | **disable** | **enable**} *guest_lan_id*}

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
guest_lan_id	LAN identifier between 1 and 5 (inclusive).
web-passthrough	Specifies the web captive portal with no authentication required.
email-input	Configures the web captive portal using an e-mail address.

Command Default

The default security policy for the wired guest LAN is web authentication.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the security web authentication policy for guest LAN ID 1:

```
(Cisco Controller) > config guest-lan security web-auth enable 1
```

Related Commands

config ingress-interface guest-lan

config guest-lan create

config interface guest-lan

config interface 3g-vlan

To configure 3G/4G-VLAN interface, use the **config interface 3g-vlan** command.

config interface 3g-vlan *interface-name* {**enable** | **disable**}

Syntax Description

interface-name **enable**	Enables the specified 3G/4G-VLAN interface
interface-name **disable**	Disables the specified 3G/4G-VLAN interface

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to configure 3G/4G-VLAN interface,:

```
(Cisco Controller) > config interface 3g-vlan vlan-int enable
```

config interface acl

To configure access control list of an interface, use the **config interface acl** command.

config interface acl {**ap-manager** | **management** | *interface_name*} {*ACL* | **none**}

Syntax Description

ap-manager	Configures the access point manager interface.
management	Configures the management interface.
interface_name	Interface name.
ACL	ACL name up to 32 alphanumeric characters.
none	Specifies none.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an access control list with a value None:

```
(Cisco Controller) > config interface acl management none
```

config interface address

To configure address information for an interface, use the **config interface address** command.

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* }

Syntax Description

ap-manager	Specifies the access point manager interface.
IP_address	IP address— IPv4 only.
netmask	Network mask.
gateway	IP address of the gateway.
management	Specifies the management interface.
service-port	Specifies the out-of-band service port interface.
virtual	Specifies the virtual gateway interface.
interface-name	Specifies the interface identified by the *interface-name* parameter.
interface-name	Interface name.
redundancy-management	Configures redundancy management interface IP address.
peer-redundancy-management	Configures the peer redundancy management interface IP address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For Cisco 5500 Series Controllers, you are not required to configure an AP-manager interface. The management interface acts like an AP-manager interface by default.

This command is applicable for IPv4 addresses only.

Ensure that the management interfaces of both controllers are in the same subnet. Ensure that the Redundant Management IP address for both controllers is the same. Likewise, ensure that the Peer Redundant Management IP address for both the controllers is the same.

The following example shows how to configure an access point manager interface with IP address 209.165.201.31, network mask 255.255.0.0, and gateway address 209.165.201.30:

```
(Cisco Controller) > config interface address ap-manager 209.165.201.31 255.255.0.0
209.165.201.30
```

The following example shows how to configure a redundancy management interface on the controller:

```
(Cisco Controller) > config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 192.0.2.1
```

Related Commands

show interface

config interface address redundancy-management

To configure the management interface IP address, subnet and gateway of the controller, use the **config interface address redundancy-management** command.

config interface address redundancy-management *IP_address netmask gateway*

Syntax Description

IP_address	Management interface IP address of the active controller.
netmask	Network mask.
gateway	IP address of the gateway.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command to check the Active-Standby reachability when the keep-alive fails.

The following example shows how to configure the management IP addresses of the controller:

```
(Cisco Controller) > config interface address redundancy-management 209.165.201.31 255.255.0.0
 209.165.201.30
```

Related Commands

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

To enable or disable access point manager features on the management or dynamic interface, use the **config interface ap-manager** command.

config interface ap-manager {**management** | *interface_name*} {**enable** | **disable**}

Syntax Description

management	Specifies the management interface.
interface_name	Dynamic interface name.
enable	Enables access point manager features on a dynamic interface.
disable	Disables access point manager features on a dynamic interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **management** option to enable or disable dynamic AP management for the management interface. For Cisco 5500 Series Controllers, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

When you enable this feature for a dynamic interface, the dynamic interface is configured as an AP-manager interface (only one AP-manager interface is allowed per physical port). A dynamic interface that is marked as an AP-manager interface cannot be used as a WLAN interface.

The following example shows how to disable an access point manager myinterface:

```
(Cisco Controller) > config interface ap-manager myinterface disable
```

config interface create

To create a dynamic interface (VLAN) for wired guest user access, use the **config interface create** command.

config interface create *interface_name vlan-id*

Syntax Description

interface_name	Interface name.
vlan-id	VLAN identifier.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a dynamic interface with the interface named lab2 and VLAN ID 6:

```
(Cisco Controller) > config interface create lab2 6
```

config interface delete

To delete a dynamic interface, use the **config interface delete** command.

config interface delete *interface-name*

Syntax Description

interface-name	*interface-name*Interface name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a dynamic interface named VLAN501:

```
(Cisco Controller) > config interface delete VLAN501
```

config interface dhcp management

To configure DHCP options on a mangament interface, use the **config interface dhcp management** command.

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**} }

Syntax Description

option-82	Configures DHCP Option 82 on the interface.
bridge-mode-insertion	Configures DHCP option 82 insertion in bridge mode.
disable	Disables the feature.
enable	Enables the feature.
linksel	Configures link select suboption 5 on a dynamic or management interface.
relaysrc	Configures Link select suboption 5 on relay source.
interface-name	Name of an existing controller interface reachable from the DHCP server.
vpnid	Configures VPN select suboption 151 VPN Id.
vpn-id	VPN Id in oui:vpn-index format xxxxxx:xxxxxxxx.
vrfname	Configures VPN select suboption 151 VRF name.
vrf-name	VRF name as string of length 7.
primary	Specifies the primary DHCP server.
primary-dhcp-server	IP address of the server.
secondary	(Optional) Specifies the secondary DHCP server.
secondary-dhcp-server	IP address of the server.
proxy-mode	Configures the DHCP proxy mode on the interface.
global	Uses the global DHCP proxy mode on the interface.
disable	(Optional) Disables the DHCP proxy mode on the interface.
global	(Optional) Uses the global DHCP proxy mode on the interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The new keywords **linksel** and **vpnsel** are added. This command supports IPv6 from this release.

Usage Guidelines

DHCP proxy is not supported for IPv6 and it works in disabled mode.

The following example shows how to configure option 82 on a management interface.

```
(Cisco Controller) > config interface dhcp management option-82 enable
```

Related Commands

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

Configure DHCP Option 82 insertion in Bridge mode on either management interface or dynamic interface by entering the **config interface dhcp** command:

config interface dhcp {**management** | **dynamic-interface** *dynamic-interface-name*} **option-82 bridge-mode-insertion** {**enable** | **disable**}

Syntax Description

management	Management interface
dynamic-interface	Dynamic interface
dynamic-interface-name	Dynamic interface name
option-82	DHCP Option 82 on the interface
bridge-mode-insertion	To configure Bridge mode insertion

Command Default

DHCP option 82 insertion in Bridge mode is disabled.

Command History

Release	Modification
8.0	The Bridge mode insertion parameter was introduced in this release.

config interface dhcp dynamic-interface

To configure the DHCP option 6 override on the interface to use OpenDNS server IPs or not, use the **config interface dhcp dynamic-interface**command.

config interface dhcp dynamic-interface *intf-name* **option-6-opendns** { **enable** | **disable** }

Syntax Description

intf-name	Interface name.
enable	Enables the DHCP option 6 override on the interface with OpenDNS IP address as default.
disable	Disables the DHCP option 6 override on the interface and DHCP provided DNS IPs will be used..

Command Default

None

Command Modes

Controller Config >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure the DHCP option 6 override on the interface to use OpenDNS server IPs:

```
(Cisco Controller) > config interface dhcp management option-6-opendns enable
```

config interface dhcp management option-6-opendns

To configure the DHCP Option 6 override on the interface in order to use OpenDNS server IPs, use the **config interface dhcp management option-6-opendns** command.

config interface dhcp management option-6-opendns { **enable** | **disable** }

Syntax Description

enable	Enables the DHCP Option 6 override on the interface, with the OpenDNS IP address as the default.
disable	Disables the DHCP Option 6 override on the interface, and uses the DHCP-provided DNS IPs.

Command Default

DHCP Option 6 override is not enabled.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to configure the DHCP Option 6 override on the interface in order to use OpenDNS server IPs:

```
(Cisco Controller) > config interface dhcp management option-6-opendns enable
```

config interface address

To configure interface addresses, use the **config interface address** command.

config interface address {**dynamic-interface** *dynamic_interface netmask gateway* | **management** | **redundancy-management** *IP_address* **peer-redundancy-management** | **service-port** *netmask* | **virtual**} *IP_address*

Syntax Description

dynamic-interface	Configures the dynamic interface of the controller.
dynamic_interface	Dynamic interface of the controller.
IP_address	IP address of the interface.
netmask	Netmask of the interface.
gateway	Gateway of the interface.
management	Configures the management interface IP address.
redundancy-management	Configures redundancy management interface IP address.
peer-redundancy-management	Configures the peer redundancy management interface IP address.
service-port	Configures the out-of-band service port.
virtual	Configures the virtual gateway interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Ensure that the management interfaces of both controllers are in the same subnet. Ensure that the redundant management IP address for both controllers is the same and that the peer redundant management IP address for both the controllers is the same.

The following example shows how to configure a redundancy management interface on the controller:

```
 (Cisco Controller) >config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

The following example shows how to configure a virtual interface:

```
(Cisco Controller) > config interface address virtual 10.10.10.1
```

Related Commands

show interface group summary

show interface summary

config interface group failure-detect

To configure failure detection mode for an interface group, use the **config interface group failure-detect** command.

config interface group failure-detect *interface group name* { **aggressive** | **non-aggressive** }

Syntax Description

interface-group-name	Name of the interface group to enable the failure-detect mode. The interface group name can be up to 32 case-sensitive, alphanumeric characters.
aggressive	The interface is marked as dirty if a client fails to get an IP from the DHCP server on this VLAN.
non-aggressive	The interface is marked as dirty if a minimum of 3 different clients fail to get an IP on this VLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

None

The following example shows how to enable failure-detect, aggressive mode for an interface group floor1:

```
(Cisco Controller) > config interface group failure-detect floor1 aggressive
```

config interface group mdns-profile

To configure an mDNS (multicast DNS) profile for an interface group, use the **config interface group mdns-profile** command.

config interface group mdns-profile {**all** | *interface-group-name*} {*profile-name* | **none**}

Syntax Description

all	Configures an mDNS profile for all interface groups.
interface-group-name	Name of the interface group to which the mDNS profile has to be associated. The interface group name can be up to 32 case-sensitive, alphanumeric characters.
profile-name	Name of the mDNS profile.
none	Removes all existing mDNS profiles from the interface group. You cannot configure mDNS profiles on the interface group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If the mDNS profile is associated to a WLAN, an error appears.

The following example shows how to configure an mDNS profile for an interface group floor1:

```
(Cisco Controller) > config interface group mdns-profile floor1 profile1
```

Related Commands

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 guest-lan

To enable or disable the guest LAN VLAN, use the **config interface guest-lan** command.

config interface guest-lan *interface_name* {*enable* | *disable*}

Syntax Description

interface_name	Interface name.
enable	Enables the guest LAN.
disable	Disables the guest LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the guest LAN feature on the interface named myinterface:

```
(Cisco Controller) > config interface guest-lan myinterface enable
```

Related Commands

config guest-lan create

config interface hostname

To configure the Domain Name System (DNS) hostname of the virtual gateway interface, use the **config interface hostname** command.

config interface hostname virtual *DNS_host*

Syntax Description

virtual	Specifies the virtual gateway interface to use the specified virtual address of the fully qualified DNS name. The virtual gateway IP address is any fictitious, unassigned IP address, such as 192.0.2.1, to be used by Layer 3 security and mobility managers.
DNS_host	DNS hostname.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure virtual gateway interface to use the specified virtual address of the fully qualified DNS hostname DNS_Host:

```
(Cisco Controller) > config interface hostname virtual DNS_Host
```

config interface nasid

To configure the Network Access Server identifier (NAS-ID) for the interface, use the **config interface nasid** command.

config interface nasid {*NAS-ID* | **none**} *interface_name*

Syntax Description

NAS-ID	Network Access Server identifier (NAS-ID) for the interface. The NAS-ID is sent to the RADIUS server by the controller (as a RADIUS client) using the authentication request, which is used to classify users to different groups. You can enter up to 32 alphanumeric characters. Beginning in Release 7.4 and later releases, you can configure the NAS-ID on the interface, WLAN, or an access point group. The order of priority is AP group NAS-ID > WLAN NAS-ID > Interface NAS-ID.
none	Configures the controller system name as the NAS-ID.
interface_name	Interface name up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

The following example shows how to configure the NAS-ID for the interface:

```
(Cisco Controller) > config interface nasid
```

Related Commands

config wlan nasid

config wlan apgroup

config interface nat-address

To deploy your Cisco 5500 Series Controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT), use the **config interface nat-address** command.

config interface nat-address {**management** | **dynamic-interface** *interface_name*} {{**enable** | **disable**} | {**set** *public_IP_address*}}

Syntax Description

management	Specifies the management interface.
dynamic-interface *interface_name*	Specifies the dynamic interface name.
enable	Enables one-to-one mapping NAT on the interface.
disable	Disables one-to-one mapping NAT on the interface.
public_IP_address	External NAT IP address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

These NAT commands can be used only on Cisco 5500 Series Controllers and only if the management interface is configured for dynamic AP management.

These commands are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. They do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

The following example shows how to enable one-to-one mapping NAT on the management interface:

```
(Cisco Controller) > config interface nat-address management enable
```

The following example shows how to set the external NAP IP address 10.10.10.10 on the management interface:

```
(Cisco Controller) > config interface nat-address management set 10.10.10.10
```

config interface port

To map a physical port to the interface (if a link aggregation trunk is not configured), use the **config interface port** command.

config interface port {**management** | *interface_name* | **redundancy-management**} *primary_port* [*secondary_port*]

Syntax Description

management	Specifies the management interface.
interface_name	Interface name.
redundancy-management	Specifies the redundancy management interface.
primary_port	Primary physical port number.
secondary_port	(Optional) Secondary physical port number.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use the **management** option for all controllers except the Cisco 5500 Series Controllers.

The following example shows how to configure the primary port number of the LAb02 interface to 3:

```
(Cisco Controller) > config interface port lab02 3
```

config interface quarantine vlan

To configure a quarantine VLAN on any dynamic interface, use the **config interface quarantine vlan** command.

config interface quarantine vlan *interface-name vlan_id*

Syntax Description

interface-name	Interface's name.
vlan_id	VLAN identifier. **Note** Enter 0 to disable quarantine processing.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a quarantine VLAN on the quarantine interface with the VLAN ID 10:

```
(Cisco Controller) > config interface quarantine vlan quarantine 10
```

config interface url-acl

To Configures an interface's URL Access Control List, use the **config interface url-acl**command.

config interface url-acl {**management** | *interface_name*} {*acl-name* | **none**}

Syntax Description

management	Configures the management interface.
interface_name	Interface name.
acl-name	ACL name up to 32 alphanumeric characters.
none	Disable the acl configured on the interface.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to configure an interface's url acl:

```
(Cisco Controller) >config interface url-acl management test
```

config interface vlan

To configure an interface VLAN identifier, use the **config interface vlan** command.

config interface vlan {**ap-manager** | **management** | *interface-name* | **redundancy-management**} *vlan*

Syntax Description

ap-manager	Configures the access point manager interface.
management	Configures the management interface.
interface_name	Interface name.
vlan	VLAN identifier.
redundancy-management	Specifies the redundancy management interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot change the redundancy management VLAN when the system redundancy management interface is mapped to the redundancy port. You must configure the redundancy management port first.

The following example shows how to configure VLAN ID 10 on the management interface:

```
(Cisco Controller) > config interface vlan management 10
```

config interface mdns-profile

To configure an mDNS (multicast DNS) profile for an interface, use the **config interface mdns-profile** command.

config interface mdns-profile {**management** | **all** *interface-name*} {*profile-name* | **none**}

Syntax Description

management	Configures an mDNS profile for the management interface.
all	Configures an mDNS profile for all interfaces.
interface-name	Name of the interface on which the mDNS profile has to be configured. The interface name can be up to 32 case-sensitive, alphanumeric characters.
profile-name	Name of the mDNS profile.
none	Removes all existing mDNS profiles from the interface. You cannot configure mDNS profiles on the interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If the mDNS profile is associated to a WLAN, an error appears.

The following example shows how to configure an mDNS profile for an interface lab1:

```
(Cisco Controller) > config interface mdns-profile lab1 profile1
```

Related Commands

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

To delete an icon or icons from flash, use the **config icons delete** command in the WLAN configuration mode.

config icons delete { *filename* | **all** }

Syntax Description

filename	Name of the icon to be deleted.
all	Deletes all the icon files from the system.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

The following example shows how to delete an icon from flash:

```
Cisco Controller > config icons delete image-1
```

config icons file-info

To configure an icon parameter, use the **config icons file-info** command in WLAN configuration mode.

config icons file-info *filename file-type lang-code width height*

Syntax Description

filename	Icon filename. It can be up to 32 characters long.
file-type	Icon filename type or extension. It can be up to 32 characters long.
lang-code	Language code of the icon. Enter 2 or 3 letters from ISO-639, for example: *eng* for English.
width	Icon width. The range is from 1 to 65535.
height	Icon height. The range is from 1 to 65535.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure icon parameters:

```
Cisco Controller > config icons file-info ima png eng 300 200
```

config ipv6 disable

To disable IPv6 globally on the controller, use the **config ipv6 disable** command .

config ipv6 disable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the IPv6 configuration is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you use this command, the controller drops all IPv6 packets and the clients will not receive any IPv6 address.

The following example shows how to disable IPv6 on the controller:

```
(Cisco Controller) >config ipv6 disable
```

config ipv6 enable

To enable IPv6 globally on the controller, use the **config ipv6 enable** command.

config ipv6 enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the IPv6 configuration is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable IPv6 on the controller:

```
(Cisco Controller) >config ipv6 enable
```

config ipv6 acl

To create or delete an IPv6 ACL on the Cisco wireless LAN controller, apply ACL to data path, and configure rules in the IPv6 ACL, use the **config ipv6 acl** command.

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*

Syntax Description

apply *name*	Applies an IPv6 ACL. An IPv6 ACL can contain up to 32 alphanumeric characters.
cpu *name*	Applies the IPv6 ACL to the CPU.
cpu none	Configure none if you wish not to have a IPV6 ACL.
create	Creates an IPv6 ACL.
delete	Deletes an IPv6 ACL.
rule（**action**） （*name*） （*index*）	Configures rules in the IPv6 ACL to either permit or deny access. IPv6 ACL name can contains up to 32 alphanumeric characters and IPv6 ACL rule index can be between 1 and 32.
{**permit**	**deny**}	Permit or deny the IPv6 rule action.
add *name index*	Adds a new rule and rule index.
change *name old_index new_index*	Changes a rule's index.
delete *name index*	Deletes a rule and rule index.
destination address *name index ip_addr prefix-len*	Configures a rule's destination IP address and prefix length (between 0 and 128).

destination port *name index*	Configure a rule's destination port range. Enter IPv6 ACL name and set an rule index for it.
direction *name index* {**in** | **out** | **any**}	Configures a rule's direction to in, out, or any.
dscp *name index dscp*	Configures a rule's DSCP. For rule index of DSCP, select a number between 0 and 63, or **any**.
protocol *name index protocol*	Configures a rule's protocol. Enter a name and set an index between 0 and 255 or **any**
source address *name index ip_address prefix-len*	Configures a rule's source IP address and netmask.
source port range *name index start_port end_port*	Configures a rule's source port range.
swap index *name index_1 index_2*	Swap's two rules' indices.

Command Default

After adding an ACL, the **config ipv6 acl cpu** is by default configured as **enabled**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6..
8.0	This command was updated by adding **cpu** and **none** keywords and the *ipv6_acl_name* variable.

Usage Guidelines

For a Cisco 2100 Series Wireless LAN Controller, you must configure a preauthentication ACL on the wireless LAN for the external web server. This ACL should then be set as a wireless LAN preauthentication ACL under Web Policy. However, you do not need to configure any preauthentication ACL for Cisco 4400 Series Wireless LAN Controllers.

The following example shows how to configure an IPv6 ACL to permit access:

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

The following example shows how to configure an interface ACL:

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

Related Commands

show ipv6 acl detailed

show ipv6 acl cpu

config ipv6 capwap

To enable or disable an IPv6 CAPWAP UDPLite for CAPWAP AP on the controller, use the **config ipv6 capwap** command.

config ipv6 capwap udplite { **enable** | **disable** } [**all** | *cisco-ap*]

Syntax Description

udplite	Configure IPv6 for CAPWAP UDP Lite.
enable	Enables IPv6 CAPWAP UDP Lite.
disable	Disables IPv6 CAPWAP UDP Lite.
all	Enables or disables IPv6 CAPWAP UDP Lite on all Cisco APs.
cisco-ap	Enables or disables IPv6 CAPWAP UDP Lite on the user defined Cisco AP.

Command Default

The **config ipv6 capwap udplite** command is by default configured as **enabled**.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0

Usage Guidelines

- IPv6 CAPWAP UDP Lite configuration applies only to APs that are connected to controller using IPv6 tunnel.
- For APs connected to controller using IPv4 Tunnel, IPv6 CAPWAP UDPLite command will not apply on either global configuration or on Per AP.
- IPv6 mandates complete payload checksum for UDP and this will have performance implications. To minimize the impact, UDPLite (mandates only header checksum) will be used for data traffic and UDP for control traffic.
- Usage UDP Lite will have an impact on the firewall. Intermediate firewall must be configured to allow UDP Lite protocol (protocol ID of 136) packets.
- Turning off UDP Lite will cause performance issues on packet handling.
- Changing from UDP to UDPLite or vice-versa will enforce the AP to disjoin and re-join.

The following example shows how to configure an IPv6 CAPWAP UDP Lite on All Cisco APs or on a particular Cisco AP:

```
(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

To configure IPv6 system interfaces, use the **config ipv6 interface**command.

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**]

Syntax Description

acl	Configures IPv6 on an interface's Access Control List.
management	Configures the management interface.
acl_name	Enter IPv6 ACL name for the management ACL. It supports up to 32 alphanumeric characters.
address	Configures IPv6 on an interface's address information.
management	Configures the management interface.
primary	Configures the primary IPv6 Address for an interface
ipv6_address	Configures an interface with IPv6 address information.
prefix_length	Configures IPv6 Prefix length. The range for prefix length is 1 to 127.
ipv6_gateway_address	Configures the Link Layer IPv6 gateway Address.
service-port	Configures IPv6 on the out-of-band service Port.
ipv6_address	Configures an interface with IPv6 address information.
prefix_length	Configures IPv6 Prefix length. The range for prefix length is 1 to 127.
slacc	Configures SLAAC options on an interface.
service-port	Configures IPv6 on the out-of-band service Port.
enable	Enables SLAAC Option
disable	Disables SLAAC Option

Command Default

None.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0.

The following example shows how to configure an IPv6 ACL management interface:

```
(Cisco Controller) >config ipv6 interface acl management Test_ACL
```

The following example shows how to configure an IPv6 address and primary interface:

```
(Cisco Controller) > config ipv6 interface address management primary 2001:9:10:56::44 64
fe80::aea0:16ff:fe4f:2244
```

Related Commands

show interface detailed management

show ipv6 interface summary

config ipv6 multicast

To configure IPv6 multicast, use the **config ipv6 multicast** command.

config ipv6 multicast mode {**unicast** | **multicast** *ipv6_address*}

Syntax Description

mode	Configure the controller to AP Multicast or Broadcast IPv6 traffic forwarding mode.
unicast	Multicast/Broadcast IPv6 packets are encapsulated in unicast CAPWAP tunnel to AP.
multicast	Multicast/Broadcast IPv6 packets are encapsulated in multicast CAPWAP tunnel to AP.
ipv6_address	Configures IPv6 multicast address.

Command Default

- By default, multicast is enabled on Cisco 8500 and 2500 Series Wireless Controllers.
- By default, unicast is enabled on Cisco 5500 Series Wireless Controllers.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0.

Usage Guidelines

none...

The following example shows how to configure an IPv6 multicast on the controller, to permit access:

```
(Cisco Controller) >config ipv6 multicast 2001:DB8:0000:0000:0000:0000:0000:0001
```

The following example shows how to configure an IPv6 unicast on the controller, to permit access:

```
(Cisco Controller) > config ipv6 multicast mode unicast
```

Related Commands

show network summary

config ipv6 neighbor-binding

To configure the Neighbor Binding table on the Cisco wireless LAN controller, use the **config ipv6 neighbor-binding** command.

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*} }

Syntax Description

timers	Configures the neighbor binding table timeout timers.
down-lifetime	Configures the down lifetime.
down_time	Down lifetime in seconds. The range is from 0 to 86400. The default is 30 seconds.
reachable-lifetime	Configures the reachable lifetime.
reachable_time	Reachable lifetime in seconds. The range is from 0 to 86400. The default is 300 seconds.
stale-lifetime	Configures the stale lifetime.
stale_time	Stale lifetime in seconds. The range is from 0 to 86400. The default is 86400 seconds.
ra-throttle	Configures IPv6 RA throttling options.
allow	Specifies the number of multicast RAs per router per throttle period.
at_least_value	Number of multicast RAs from router before throttling. The range is from 0 to 32. The default is 1.
enable	Enables IPv6 RA throttling.
disable	Disables IPv6 RA throttling.
interval-option	Adjusts the behavior on RA with RFC3775 interval option.
ignore	Indicates interval option has no influence on throttling.
passthrough	Indicates all RAs with RFC3775 interval option will be forwarded (default).
throttle	Indicates all RAs with RFC3775 interval option will be throttled.

max-through	Specifies unthrottled multicast RAs per VLAN per throttle period.
no_mcast_RA	Number of multicast RAs on VLAN by which throttling is enforced. The default multicast RAs on vlan is 10.
no-limit	Configures no upper bound at the VLAN level.
throttle-period	Configures the throttle period.
throttle_period	Duration of the throttle period in seconds. The range is from 10 to 86400 seconds. The default is 600 seconds.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Neighbor Binding table:

```
(Cisco Controller) >config ipv6 neighbor-binding ra-throttle enable
```

Related Commands

show ipv6 neighbor-binding

config ipv6 ns-mcast-fwd

To configure the nonstop multicast cache miss forwarding, use the **config ipv6 ns-mcast-fwd** command.

config ipv6 ns-mcast-fwd {**enable** | **disable**}

Syntax Description

enable	Enables nonstop multicast forwarding on a cache miss.
disable	Disables nonstop multicast forwarding on a cache miss.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an nonstop multicast forwarding:

```
(Cisco Controller) >config ipv6 ns-mcast-fwd enable
```

config ipv6 ra-guard

To configure the filter for Router Advertisement (RA) packets that originate from a client on an AP, use the **config ipv6 ra-guard** command.

config ipv6 ra-guard ap {**enable** | **disable**}

Syntax Description

enable	Enables RA guard on an AP.
disable	Disables RA guard on an AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable IPv6 RA guard:

```
(Cisco Controller) >config ipv6 ra-guard enable
```

Related Commands

show ipv6 ra-guard

config ipv6 route

To add or delete an IPv6 network route, use the **config ipv6 route**command.

config ipv6 route {**add** *network_ipv6_addr prefix-len ipv6_gw_addr* | **delete** *network _ipv6 addr* }

Syntax Description

add	Adds an IPv6 network route.
network_ipv6_addr	Enter the networks IPv6 address.
prefix-len	Enter the prefix length for the network.
ipv6_gw_addr	Configures the system interfaces.
delete	Deletes an IPv6 network route.
network_ipv6_addr	Enter the networks IPv6 address.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced in Release 8.0.

Usage Guidelines

- This command is used to add and delete an IPv6 network route to access service interface over IPv6 from different network.
- While adding IPv6 route, IPv6 Gateway Address must be a link local scope (FE80::/64).

The following example shows how to add an IPv6 route:

```
(Cisco Controller) > config ipv6 route add 3010:1111:2222:abcd:abcd:abcd:abcd:1111 64
fe80::6616:8dff:fed3:c0cf
```

The following example shows how to delete an IPv6 route:

```
(Cisco Controller) > config ipv6 route delete 2001:9:5:90::115
```

Related Commands

show ipv6 route summary

Config Commands: j to q

- config known ap, on page 557
- config lag, on page 558
- config ldap, on page 559
- config local-auth active-timeout, on page 561
- config local-auth cipher-option, on page 562
- config local-auth eap-profile, on page 563
- config local-auth method fast, on page 565
- config local-auth user-credentials, on page 567
- config lync-sdn, on page 568
- config licensing, on page 569
- config license boot, on page 570
- config load-balancing, on page 571
- config location, on page 573
- config location info rogue, on page 575
- config logging buffered, on page 576
- config logging console, on page 577
- config logging debug, on page 578
- config logging fileinfo, on page 579
- config logging procinfo, on page 580
- config logging traceinfo, on page 581
- config logging syslog host, on page 582
- config logging syslog facility, on page 585
- config logging syslog facility client, on page 587
- config logging syslog facility ap, on page 588
- config logging syslog ipsec, on page 589
- config logging syslog ipsec profile, on page 590
- config logging syslog tls, on page 591
- config logging syslog level, on page 592
- config loginsession close, on page 593
- config macfilter , on page 594
- config macfilter description, on page 595
- config macfilter interface, on page 596
- config macfilter ip-address, on page 597

- config macfilter mac-delimiter, on page 598
- config macfilter radius-compat, on page 599
- config macfilter wlan-id, on page 600
- config mdns ap, on page 601
- config mdns profile, on page 602
- config mdns query interval, on page 604
- config mdns service , on page 605
- config mdns snooping , on page 607
- config mdns policy enable , on page 608
- config mdns policy service-group, on page 609
- config mdns policy service-group parameters, on page 610
- config mdns policy service-group user-name, on page 611
- config mdns policy service-group user-role, on page 612
- config media-stream multicast-direct, on page 613
- config media-stream message, on page 614
- config media-stream add, on page 615
- config media-stream admit, on page 617
- config media-stream deny, on page 618
- config media-stream delete, on page 619
- config memory monitor errors, on page 620
- config memory monitor leaks, on page 621
- config mesh alarm, on page 623
- config mesh astools, on page 624
- config mesh backhaul rate-adapt, on page 625
- config mesh backhaul slot, on page 626
- config mesh battery-state, on page 627
- config mesh client-access, on page 628
- config mesh ethernet-bridging allow-bpdu, on page 629
- config mesh ethernet-bridging vlan-transparent, on page 630
- config mesh full-sector-dfs, on page 631
- config mesh linkdata, on page 632
- config mesh linktest, on page 634
- config mesh lsc, on page 637
- config mesh lsc advanced, on page 638
- config mesh lsc advanced ap-provision, on page 639
- config mesh multicast, on page 640
- config mesh parent preferred, on page 642
- config mesh public-safety, on page 643
- config mesh radius-server, on page 644
- config mesh range, on page 645
- config mesh secondary-backhaul, on page 646
- config mesh security, on page 647
- config mesh slot-bias, on page 649
- config mgmtuser add, on page 650
- config mgmtuser delete, on page 651
- config mgmtuser description, on page 652

- config mgmtuser password, on page 653
- config mgmtuser telnet, on page 654
- config mgmtuser termination-interval, on page 655
- config mobility dscp, on page 656
- config mobility encryption tunnel, on page 657
- config mobility group anchor, on page 658
- config mobility group domain, on page 659
- config mobility group keepalive count, on page 660
- config mobility group keepalive interval, on page 661
- config mobility group member, on page 662
- config mobility group multicast-address, on page 664
- config mobility multicast-mode, on page 665
- config mobility new-architecture, on page 666
- config mobility oracle, on page 667
- config mobility secure-mode, on page 668
- config mobility statistics reset, on page 669
- config netuser add , on page 670
- config netuser delete, on page 672
- config netuser description, on page 673
- config netuser guest-lan-id, on page 674
- config netuser guest-role apply, on page 675
- config netuser guest-role create, on page 676
- config netuser guest-role delete, on page 677
- config netuser guest-role qos data-rate average-data-rate, on page 678
- config netuser guest-role qos data-rate average-realtime-rate, on page 679
- config netuser guest-role qos data-rate burst-data-rate, on page 680
- config netuser guest-role qos data-rate burst-realtime-rate, on page 681
- config netuser lifetime, on page 682
- config netuser maxUserLogin, on page 683
- config netuser password, on page 684
- config netuser wlan-id, on page 685
- config network bridging-shared-secret, on page 686
- config network web-auth captive-bypass, on page 687
- config network web-auth port, on page 688
- config network web-auth proxy-redirect, on page 689
- config network web-auth secureweb, on page 690
- config network webmode, on page 691
- config network web-auth, on page 692
- config network 802.3-bridging, on page 693
- config network allow-old-bridge-aps, on page 694
- config network ap-discovery, on page 695
- config network ap-easyadmin, on page 696
- config network ap-fallback, on page 697
- config network ap-priority, on page 698
- config network apple-talk, on page 699
- config network arptimeout, on page 700

- config assisted-roaming, on page 701
- config network allow-old-bridge-aps, on page 702
- config network ap-discovery, on page 703
- config network ap-fallback, on page 704
- config network ap-priority, on page 705
- config network apple-talk, on page 706
- config network bridging-shared-secret, on page 707
- config network bridging-shared-secret, on page 708
- config network broadcast, on page 709
- config network fast-ssid-change, on page 710
- config network ip-mac-binding, on page 711
- config network link local bridging, on page 712
- config network master-base, on page 713
- config network mgmt-via-wireless, on page 714
- config network multicast global, on page 715
- config network multicast igmp query interval, on page 716
- config network multicast igmp snooping, on page 717
- config network multicast igmp timeout, on page 718
- config network multicast l2mcast, on page 719
- config network multicast mld, on page 720
- config network multicast mode multicast, on page 721
- config network multicast mode unicast, on page 722
- config network oeap-600 dual-rlan-ports, on page 723
- config network oeap-600 local-network, on page 724
- config network otap-mode, on page 725
- config network profiling, on page 726
- config network rf-network-name, on page 727
- config network secureweb, on page 728
- config network secureweb cipher-option, on page 729
- config network ssh, on page 730
- config network telnet, on page 731
- config network usertimeout, on page 732
- config network web-auth captive-bypass, on page 733
- config network web-auth cmcc-support, on page 734
- config network web-auth port, on page 735
- config network web-auth proxy-redirect, on page 736
- config network web-auth secureweb, on page 737
- config network web-auth https-redirect, on page 738
- config network webmode, on page 739
- config network web-auth, on page 740
- config network zero-config, on page 741
- config network master-base, on page 742
- config network oeap-600 dual-rlan-ports, on page 743
- config network oeap-600 local-network, on page 744
- config network otap-mode, on page 745
- config network zero-config, on page 746

- config nmsp notify-interval measurement, on page 747
- config opendns, on page 748
- config opendns api-token , on page 749
- config opendns forced , on page 750
- config opendns profile, on page 751
- config pmipv6 domain, on page 752
- config pmipv6 add profile, on page 753
- config pmipv6 delete, on page 754
- config pmipv6 mag apn, on page 755
- config pmipv6 mag binding init-retx-time, on page 756
- config pmipv6 mag binding lifetime, on page 757
- config pmipv6 mag binding max-retx-time, on page 758
- config pmipv6 mag binding maximum, on page 759
- config pmipv6 mag binding refresh-time, on page 760
- config pmipv6 mag bri delay, on page 761
- config pmipv6 mag bri retries, on page 762
- config pmipv6 mag lma, on page 763
- config pmipv6 mag replay-protection, on page 764
- config port power, on page 765
- config policy action opendns-profile-name , on page 766
- config paging, on page 767
- config passwd-cleartext, on page 768
- config policy, on page 769
- config policy match role, on page 771
- config port adminmode, on page 772
- config port maxspeed, on page 773
- config port linktrap, on page 774
- config port multicast appliance, on page 775
- config prompt, on page 776
- config qos average-data-rate, on page 777
- config qos average-realtime-rate, on page 778
- config qos burst-data-rate, on page 779
- config qos burst-realtime-rate, on page 780
- config qos description, on page 781
- config qos fastlane, on page 782
- config qos fastlane disable global, on page 783
- config qos max-rf-usage, on page 784
- config qos dot1p-tag, on page 785
- config qos priority, on page 786
- config qos protocol-type, on page 788
- config qos queue_length, on page 789
- config qos qosmap, on page 790
- config qos qosmap up-to-dscp-map, on page 791
- config qos qosmap dscp-to-up-exception, on page 792
- config qos qosmap delete-dscp-exception, on page 793
- config qos qosmap clear-all, on page 794

• config qos qosmap trust dscp upstream, on page 795

config known ap

To configure a known Cisco lightweight access point, use the **config known ap** command.

config known ap {**add** | **alert** | **delete**} *MAC*

Syntax Description

add	Adds a new known access point entry.
alert	Generates a trap upon detection of the access point.
delete	Deletes an existing known access point entry.
MAC	MAC address of the known Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a new access point entry ac:10:02:72:2f:bf on a known access point:

```
(Cisco Controller) >config known ap add ac:10:02:72:2f:bf 12
```

config lag

To enable or disable link aggregation (LAG), use the **config lag** command.

config lag {**enable** | **disable**}

Syntax Description

enable	Enables the link aggregation (LAG) settings.
disable	Disables the link aggregation (LAG) settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LAG settings:

```
(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.
```

The following example shows how to disable LAG settings:

```
(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

To configure the Lightweight Directory Access Protocol (LDAP) server settings, use the **config ldap** command.

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*}

Syntax Description

add	Specifies that an LDAP server is being added.
delete	Specifies that an LDAP server is being deleted.
enable	Specifies that an LDAP serve is enabled.
disable	Specifies that an LDAP server is disabled.
retransmit-timeout	Changes the default retransmit timeout for an LDAP server.
retry	Configures the retry attempts for an LDAP server.
user	Configures the user search parameters.
security-mode	Configures the security mode.
simple-bind	Configures the local authentication bind method.
anonymous	Allows anonymous access to the LDAP server.
authenticated	Specifies that a username and password be entered to secure access to the LDAP server.
index	LDAP server index. The range is from 1 to 17.
server_ip_address	IP address of the LDAP server.
port	Port number.
user_base	Distinguished name for the subtree that contains all of the users.

user_attr	Attribute that contains the username.
user_type	ObjectType that identifies the user.
secure	(Optional) Specifies that Transport Layer Security (TLS) is used.
retransmit-timeout	Retransmit timeout for an LDAP server. The range is from 2 to 30.
attempts	Number of attempts that each LDAP server is retried.
attr	Configures the attribute that contains the username.
base	Configures the distinguished name of the subtree that contains all the users.
type	Configures the user type.
username	Username for the authenticated bind method.
password	Password for the authenticated bind method.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The **secure** keyword was added to support secure LDAP.

Usage Guidelines

When you enable secure LDAP, the controller does not validate the server certificate.

The following example shows how to enable LDAP server index 10:

```
(Cisco Controller) > config ldap enable 10
```

Related Commands

config ldap add

config ldap simple-bind

show ldap summary

config local-auth active-timeout

To specify the amount of time in which the controller attempts to authenticate wireless clients using local Extensible Authentication Protocol (EAP) after any pair of configured RADIUS servers fails, use the **config local-auth active-timeout** command.

config local-auth active-timeout *timeout*

Syntax Description

timeout	Timeout measured in seconds. The range is from 1 to 3600.

Command Default

The default timeout value is 100 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the active timeout to authenticate wireless clients using EAP to 500 seconds:

```
(Cisco Controller) > config local-auth active-timeout 500
```

Related Commands

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

To configure the 3DES-RC4 cipher option, use the **config local-auth cipher-option** command.

config local-auth cipher-option {**enable | disable** }

Syntax Description

cipher-option	Configures the cipher option.
enable	Allows the 3DES-RC4 cipher to be enabled.
disable	Disables the 3DES-RC4 cipher.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to disable the cipher-option on the controller:

```
(Cisco Controller) > config local-auth cipher-option 3des-rc4 disable
```

config local-auth eap-profile

To configure local Extensible Authentication Protocol (EAP) authentication profiles, use the **config local-auth eap-profile** command.

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**}

Syntax Description

add	(Optional) Specifies that an EAP profile or method is being added.
delete	(Optional) Specifies that an EAP profile or method is being deleted.
profile_name	EAP profile name (up to 63 alphanumeric characters). Do not include spaces within a profile name.
cert-issuer	(For use with EAP-TLS, PEAP, or EAP-FAST with certificates) Specifies the issuer of the certificates that will be sent to the client. The supported certificate issuers are Cisco or a third-party vendor.
cisco	Specifies the Cisco certificate issuer.
vendor	Specifies the third-party vendor.
method	Configures an EAP profile method.
method	EAP profile method name. The supported methods are leap, fast, tls, and peap.
local-cert	(For use with EAP-FAST) Specifies whether the device certificate on the controller is required for authentication.
enable	Specifies that the parameter is enabled.
disable	Specifies that the parameter is disabled.
client-cert	(For use with EAP-FAST) Specifies whether wireless clients are required to send their device certificates to the controller in order to authenticate.
peer-verify	Configures the peer certificate verification options.
ca-issuer	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the incoming certificate from the client is to be validated against the Certificate Authority (CA) certificates on the controller.

cn-verify	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the common name (CN) in the incoming certificate is to be validated against the CA certificates' CN on the controller.
date-valid	(For use with EAP-TLS or EAP-FAST with certificates) Specifies whether the controller is to verify that the incoming device certificate is still valid and has not expired.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a local EAP profile named FAST01:

```
(Cisco Controller) > config local-auth eap-profile add FAST01
```

The following example shows how to add the EAP-FAST method to a local EAP profile:

```
(Cisco Controller) > config local-auth eap-profile method add fast FAST01
```

The following example shows how to specify Cisco as the issuer of the certificates that will be sent to the client for an EAP-FAST profile:

```
(Cisco Controller) > config local-auth eap-profile method fast cert-issuer cisco
```

The following example shows how to specify that the incoming certificate from the client be validated against the CA certificates on the controller:

```
(Cisco Controller) > config local-auth eap-profile method fast peer-verify ca-issuer enable
```

Related Commands

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

To configure an EAP-FAST profile, use the **config local-auth method fast** command.

config local-auth method fast {**anon-prov** [**enable** | **disable**] | **authority-id** *auth_id* **pac-ttl** *days* | **server-key** *key_value*}

Syntax Description

anon-prov	Configures the controller to allow anonymous provisioning, which allows PACs to be sent automatically to clients that do not have one during Protected Access Credentials (PAC) provisioning.
enable	(Optional) Specifies that the parameter is enabled.
disable	(Optional) Specifies that the parameter is disabled.
authority-id	Configures the authority identifier of the local EAP-FAST server.
auth_id	Authority identifier of the local EAP-FAST server (2 to 32 hexadecimal digits).
pac-ttl	Configures the number of days for the Protected Access Credentials (PAC) to remain viable (also known as the time-to-live [TTL] value).
days	Time-to-live value (TTL) value (1 to 1000 days).
server-key	Configures the server key to encrypt or decrypt PACs.
key_value	Encryption key value (2 to 32 hexadecimal digits).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the controller to allows anonymous provisioning:

```
(Cisco Controller) > config local-auth method fast anon-prov disable
```

The following example shows how to configure the authority identifier 0125631177 of the local EAP-FAST server:

```
(Cisco Controller) > config local-auth method fast authority-id 0125631177
```

The following example shows how to configure the number of days to 10 for the PAC to remain viable:

```
(Cisco Controller) > config local-auth method fast pac-ttl 10
```

Related Commands

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

To configure the local Extensible Authentication Protocol (EAP) authentication database search order for user credentials, use the **config local-auth user credentials** command.

config local-auth user-credentials {**local** [**ldap**] | **ldap** [**local**] }

Syntax Description

local	Specifies that the local database is searched for the user credentials.
ldap	(Optional) Specifies that the Lightweight Directory Access Protocol (LDAP) database is searched for the user credentials.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The order of the specified database parameters indicate the database search order.

The following example shows how to specify the order in which the local EAP authentication database is searched:

```
(Cisco Controller) > config local-auth user credentials local lda
```

In the above example, the local database is searched first and then the LDAP database.

Related Commands

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

To configure the Lync service, use the **config lync-sdn** command.

config lync-sdn {**port** *port-number*} | {**enable** | **disable**}

Syntax Description

port	Configures the Lync server port number.
port-number	Port number of the server.
enable	Enables Lync service globally.
disable	Disables Lync service globally.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable Lync service globally:

```
(Cisco Controller) >config lync-sdn enable
```

config licensing

To switch between Cisco Smart Software Licensing and RTU licensing platform, use the **config licensing** command.

config licensing {**rtu** | **smart-license**} **dns-server** *ip address*

Syntax Description

rtu	Right To Use license platform.
smart-license	Cisco Smart Software License platform.
dns-server	Configures smart software licensing dns server parameters

Command History

Release	Modification
8.2	This command was introduced.

Command Default

The Right To Use (RTU) is the default license mechanism in the device.

The following example shows how to activate Cisco Smart Software License on the controller:

```
(Cisco Controller) > config licensing smart-license dns-server 209.165.200.224
```

Note The controller needs to be rebooted to activate the change in the license platform.

config license boot

To specify the license level to be used on the next reboot of the Cisco 5500 Series Controller, use the **config license boot** command.

config license boot {**base** | **wplus** | **auto**}

Syntax Description

base	Specifies the base boot level.
wplus	Specifies the wplus boot level.
auto	Specifies the auto boot level.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you enter **auto**, the licensing software automatically chooses the license level to use on the next reboot. It generally chooses permanent licenses over evaluation licenses and wplus licenses over base licenses.

Note If you are considering upgrading from a base license to a wplus license, you can try an evaluation wplus license before upgrading to a permanent wplus license. To activate the evaluation license, you need to set the image level to wplus in order for the controller to use the wplus evaluation license instead of the base permanent license.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the license boot settings to wplus:

```
(Cisco Controller) > config license boot wplus
```

Related Commands

license install

show license in-use

license modify priority

config load-balancing

To globally configure aggressive load balancing on the controller, use the **config load-balancing** command.

config load-balancing {**window** *client_count* | **status** {**enable** | **disable**} | **denial** *denial_count*}

config load-balancing uplink-threshold *traffic_threshold*

Syntax Description

window	Specifies the aggressive load balancing client window.
client_count	Aggressive load balancing client window with the number of clients from 1 to 20.
status	Sets the load balancing status.
enable	Enables load balancing feature.
disable	Disables load balancing feature.
denial	Specifies the number of association denials during load balancing.
denial_count	Maximum number of association denials during load balancing. from 0 to 10.
uplink-threshold	Specifies the threshold traffic for an access point to deny new associations.
traffic_threshold	Threshold traffic for an access point to deny new associations. This value is a percentage of the WAN utilization measured over a 90 second interval. For example, the default threshold value of 50 triggers the load balancing upon detecting an utilization of 50% or more on an access point WAN interface.

Command Default

By default, the aggressive load balancing is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

Clients can only be load balanced across access points joined to the same controller. The WAN utilization is calculated as a percentage using the following formula: (Transmitted Data Rate (per second) + Received Data Rate (per second))/(1000Mbps TX + 1000Mbps RX) * 100

The following example shows how to enable the aggressive load-balancing settings:

```
(Cisco Controller) > config load-balancing aggressive enable
```

Related Commands

show load-balancing

config wlan load-balance

config location

To configure a location-based system, use the **config location** command.

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**}}}

Syntax Description

algorithm	**Note**	We recommend that you do not use or modify the **config location algorithm** command. It is set to optimal default values. Configures the algorithm used to average RSSI and SNR values.
simple		Specifies a faster algorithm that requires low CPU overhead but provides less accuracy.
rssi-average		Specifies a more accurate algorithm but requires more CPU overhead.
rssi-half-life	**Note**	We recommend that you do not use or modify the **config location rssi-half-life** command. It is set to optimal default values. Configures the half-life when averaging two RSSI readings.
expiry	**Note**	We recommend that you do not use or modify the **config location expiry** command. It is set to optimal default values. Configures the timeout for RSSI values.
client		(Optional) Specifies the parameter applies to client devices.
calibrating-client		(Optional) Specifies the parameter is used for calibrating client devices.
tags		(Optional) Specifies the parameter applies to radio frequency identification (RFID) tags.
rogue-aps		(Optional) Specifies the parameter applies to rogue access points.
seconds		Time value (0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, 300 seconds).
notify-threshold	**Note**	We recommend that you do not use or modify the **config location notify-threshold** command. It is set to optimal default values. Specifies the NMSP notification threshold for RSSI measurements.
threshold		Threshold parameter. The range is 0 to 10 dB, and the default value is 0 dB.
interface-mapping		Adds or deletes a new location, wireless LAN, or interface mapping element.
wlan_id		WLAN identification name.
interface_name		Name of interface to which mapping element applies.

plm	Specifies the path loss measurement (S60) request for normal clients or calibrating clients.
client	Specifies normal, noncalibrating clients.
burst_interval	Burst interval. The range is from 1 to 3600 seconds, and the default value is 60 seconds.
calibrating	Specifies calibrating clients.
uniband	Specifies the associated 802.11a or 802.11b/g radio (uniband).
multiband	Specifies the associated 802.11a/b/g radio (multiband).

Command Default

See the "Syntax Description" section for default values of individual arguments and keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the simple algorithm for averaging RSSI and SNR values on a location-based controller:

```
(Cisco Controller) > config location algorithm simple
```

Related Commands

config location info rogue

clear location rfid

clear location statistics rfid

show location

show location statistics rfid

config location info rogue

To configure info-notification for rogue service, use the **config location info rogue** command.

config location info rogue { **basic** | **extended** }

Syntax Description

basic	Configures basic rogue parameters such as mode, class, containmentlevel, numclients, firsttime, lasttime, ssid, and so on, for rogue info-notification service. **Note** Configure the basic parameters if the version of Cisco MSE is older than the version of the controller.
extended	Configures extended rogue parameters, which is basic parameters plus security type, detecting LRAD type, and so on, for rogue info-notification service.

Command History

Release	Modification
8.0	This command was introduced.

config logging buffered

To set the severity level for logging messages to the controller buffer, use the **config logging buffered** command.

config logging buffered `security_level`

Syntax Description

security_level	Security level. Choose one of the following: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the controller buffer severity level for logging messages to 4:

```
(Cisco Controller) > config logging buffered 4
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging console

To set the severity level for logging messages to the controller console, use the **config logging console** command.

config logging console *security_level*

Syntax Description

security_level	Severity level. Choose one of the following: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the controller console severity level for logging messages to 3:

```
(Cisco Controller) > config logging console 3
```

Related Commands

config logging syslog facility

config logging syslog level

show logging

config logging debug

To save debug messages to the controller buffer, the controller console, or a syslog server, use the **config logging debug** command.

config logging debug {**buffered** | **console** | **syslog**} {**enable** | **disable**}

Syntax Description

buffered	Saves debug messages to the controller buffer.
console	Saves debug messages to the controller console.
syslog	Saves debug messages to the syslog server.
enable	Enables logging of debug messages.
disable	Disables logging of debug messages.

Command Default

The **console** command is enabled and the **buffered** and **syslog** commands are disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to save the debug messages to the controller console:

```
(Cisco Controller) > config logging debug console enable
```

Related Commands

show logging

config logging fileinfo

To cause the controller to include information about the source file in the message logs or to prevent the controller from displaying this information, use the **config logging fileinfo** command.

config logging fileinfo {**enable** | **disable**}

Syntax Description

enable	Includes information about the source file in the message logs.
disable	Prevents the controller from displaying information about the source file in the message logs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the controller to include information about the source file in the message logs:

```
(Cisco Controller) > config logging fileinfo enable
```

Related Commands

show logging

config logging procinfo

To cause the controller to include process information in the message logs or to prevent the controller from displaying this information, use the **config logging procinfo** command.

config logging procinfo {**enable** | **disable**}

Syntax Description

enable	Includes process information in the message logs.
disable	Prevents the controller from displaying process information in the message logs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the controller to include the process information in the message logs:

```
(Cisco Controller) > config logging procinfo enable
```

Related Commands

show logging

config logging traceinfo

To cause the controller to include traceback information in the message logs or to prevent the controller from displaying this information, use the **config logging traceinfo** command.

config logging traceinfo {**enable** | **disable**}

Syntax Description

enable	Includes traceback information in the message logs.
disable	Prevents the controller from displaying traceback information in the message logs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the controller to include the traceback information in the message logs:

```
(Cisco Controller) > config logging traceinfo disable
```

Related Commands

show logging

config logging syslog host

To configure a remote host for sending syslog messages, use the **config logging syslog host** command.

config logging syslog host *ip_addr*

Syntax Description

ip_addr	IP address for the remote host.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- To configure a remote host for sending syslog messages, use the **config logging syslog host** *ip_addr* command.
- To remove a remote host that was configured for sending syslog messages, use the **config logging syslog host** *ip_addr* **delete** command.
- To display the configured syslog servers on the controller, use the **show logging** command.

The following example shows how to configure two remote hosts 10.92.125.52 and 2001:9:6:40::623 for sending the syslog messages and displaying the configured syslog servers on the controller:

```
(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
```

The following example shows how to remove two remote hosts 10.92.125.52 and 2001:9:6:40::623 that were configured for sending syslog messages and displaying that the configured syslog servers were removed from the controller:

```
(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

To set the facility for outgoing syslog messages to the remote host, use the **config logging syslog facility** command.

config logging syslog facility *facility_code*

Syntax Description

facility_code	Facility code. Choose one of the following: • authorization—Authorization system. Facility level—4. • auth-private—Authorization system (private). Facility level—10. • cron—Cron/at facility. Facility level—9. • daemon—System daemons. Facility level—3. • ftp—FTP daemon. Facility level—11. • kern—Kernel. Facility level—0. • local0—Local use. Facility level—16. • local1—Local use. Facility level—17. • local2—Local use. Facility level—18. • local3—Local use. Facility level—19. • local4—Local use. Facility level—20. • local5—Local use. Facility level—21. • local6—Local use. Facility level—22. • local7—Local use. Facility level—23. • lpr—Line printer system. Facility level—6. • mail—Mail system. Facility level—2. • news—USENET news. Facility level—7. • sys12—System use. Facility level—12. • sys13—System use. Facility level—13. • sys14—System use. Facility level—14. • sys15—System use. Facility level—15. • syslog—The syslog itself. Facility level—5. • user—User process. Facility level—1. • uucp—UNIX-to-UNIX copy system. Facility level—8.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the facility for outgoing syslog messages to authorization:

```
(Cisco Controller) > config logging syslog facility authorization
```

Related Commands

config logging syslog host

config logging syslog level

show logging

config logging syslog facility client

To configure the syslog facility to AP, use the **config logging syslog facility client** { **assocfail Dot11** | **associate Dot11** | **authentication** | **authfail Dot11** | **deauthenticate Dot11** | **disassociate Dot11** | **exclude**}{ **enable** | **disable**} command.

config logging syslog facility *Client*

Syntax Description

Client	Facility Client. Has the following functions: • assocfail Dot11—Association fail syslog for clients • associate Dot11—Association syslog for clients • authentication—Authentication success syslog for cli • authfail Dot11—Authentication fail syslog for clients • deauthenticate Dot11—Deauthentication syslog for cl • disassociate Dot11—Disassociation syslog for clients • excluded—Excluded syslog for clients

Command Default

None

Command History

Release	Modification
7.5	This command was introduced in a release earlier than Release 7.5.

The following example shows how to set the facility syslog facility for client:

```
cisco controller config logging syslog facility client
```

Related Commands

show logging flags client

config logging syslog facility ap

To configure the syslog facility to AP, use the **config logging syslog facility ap** { **associate** | **disassociate** } { **enable** | **disable** } command.

config logging syslog facility *AP*

Syntax Description

AP	Facility AP. Has the following functions: • associate—Association syslog for AP • disassociate—Disassociation syslog for AP

Command Default

None

Command History

Release	Modification
7.5	This command was introduced in a release earlier than Release 7.5.

The following example shows how to configure syslog facility for AP:

```
cisco controller config logging syslog facility ap
```

Related Commands

show logging flags ap

config logging syslog ipsec

To configure transmission of syslog messages over IPSec, use the **config logging syslog ipsec** command.

config logging syslog ipsec { **enable** | **disable** }

Syntax Description

enable	Enables transmission of syslog messages over IPSec.
disable	Disables transmission of syslog messages over IPSec.

Command Default

By default, transmission of syslog messages over IPSec is disabled.

Command History

Release	Modification
8.0	This command was introduced.

Examples

The following example shows how to enable transmission of syslog messages over IPSec:

```
(Cisco Controller) > config logging syslog ipsec enable
```

config logging syslog ipsec profile

To configure an IPSec profile to define IPSec parameters for the connection, use the **config logging syslog ipsec profile** command.

config logging syslog ipsec profile *profile-name*

Syntax Description

profile-name	Name of the IPSec profile to use.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Examples

The following example shows how to configure an IPSec profile name to define IPSec parameters:

```
(Cisco Controller) > config logging syslog ipsec profile ipsec-profile-1
```

config logging syslog tls

To configure transmission of syslog messages over transport layer security (TLS), use the **config logging syslog tls** command.

config logging syslog tls { **enable** | **disable** }

Syntax Description

enable	Enables transmission of syslog messages over TLS. Enabling syslog over TLS on the controller enables the feature for all syslog hosts defined in the controller. You can define up to three syslog hosts per controller. The controller transmits messages concurrently to all the configured syslog hosts.
disable	Disables transmission of syslog messages over TLS.

Command Default

By default, transmission of syslog messages over TLS is disabled.

Command History

Release	Modification
8.0	This command was introduced.

Examples

The following example shows how to enable transmission of syslog messages over TLS:

```
(Cisco Controller) > config logging syslog tls enable
```

Related Commands

show logging

config logging syslog level

To set the severity level for filtering syslog messages to the remote host, use the **config logging syslog level** command.

config logging syslog level *severity_level*

Syntax Description

severity_level	Severity level. Choose one of the following: • emergencies—Severity level 0 • alerts—Severity level 1 • critical—Severity level 2 • errors—Severity level 3 • warnings—Severity level 4 • notifications—Severity level 5 • informational—Severity level 6 • debugging—Severity level 7

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the severity level for syslog messages to 3:

```
(Cisco Controller) > config logging syslog level 3
```

Related Commands

config logging syslog host

config logging syslog facility

show logging

config loginsession close

To close all active Telnet sessions, use the **config loginsession close** command.

config loginsession close {*session_id* | **all**}

Syntax Description

session_id	ID of the session to close.
all	Closes all Telnet sessions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to close all active Telnet sessions:

```
(Cisco Controller) > config loginsession close all
```

Related Commands

show loginsession

config macfilter

To create or delete a MAC filter entry on the Cisco wireless LAN controller, use the **config macfilter** {*add* | *delete*} command.

config macfilter {**add** *client_MAC wlan_id* [*interface_name*] [*description*] [*macfilter_IP*] | **delete** *client_MAC*}

Syntax Description

add	Adds a MAC filter entry on the controller.
delete	Deletes a MAC filter entry on the controller.
MAC_addr	Client MAC address.
wlan_id	Wireless LAN identifier with which the MAC filter entry should associate. A zero value associates the entry with any wireless LAN.
interface_name	(Optional) Name of the interface. Enter **0** to specify no interface.
description	(Optional) Short description of the interface (up to 32 characters) in double quotes. **Note** A description is mandatory if *macfilterIP* is specified.
IP Address	(Optional) IPv4 address of the local MAC filter database.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use the **config macfilter add** command to add a client locally to a wireless LAN on the Cisco wireless LAN controller. This filter bypasses the RADIUS authentication process.

As on release 7.6, the optional *macfilter_IP* supports only IPv4 address.

The following example shows how to add a MAC filter entry 00:E0:77:31:A3:55 with the wireless LAN ID 1, interface name labconnect, and MAC filter IP 10.92.125.51 on the controller:

```
(Cisco Controller) > config macfilter add 00:E0:77:31:A3:55 1 lab02 "labconnect" 10.92.125.51
```

Related Commands

show macfilter

config macfilter ip-address

config macfilter description

To add a description to a MAC filter, use the **config macfilter description** command.

config macfilter description *MAC addrdescription*

Syntax Description

MAC addr	Client MAC address.
description	(Optional) Description within double quotes (up to 32 characters).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the description MAC filter 01 to MAC address 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter description 11:11:11:11:11:11 "MAC Filter 01"
```

Related Commands

show macfilter

config macfilter interface

To create a MAC filter client interface, use the **config macfilter interface** command.

config macfilter interface *MAC_addr interface*

Syntax Description

MAC addr	Client MAC address.
interface	Interface name. A value of zero is equivalent to no name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a MAC filer interface Lab01 on client 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter interface 11:11:11:11:11:11 Lab01
```

Related Commands

show macfilter

config macfilter ip-address

To enter passive client IP address , use the **config macfilter ip-address** command.

config macfilterip-address *MAC_addr IP Address*

Syntax Description

MAC_addr	MAC address of the client.
IP Address	Adds an IP address for passive clients.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4.

The following example shows how to add an IP address for a passive client:

```
(Cisco Controller) > config macfilter ip-address aa-bb-cc-dd-ee-ff 10.92.125.51
```

Related Commands

show macfilter

config macfilter mac-delimiter

To set the MAC delimiter (colon, hyphen, none, and single-hyphen) for MAC addresses sent to RADIUS servers, use the **config macfilter mac-delimiter** command.

config macfilter mac-delimiter {**none** | **colon** | **hyphen** | **single-hyphen**}

Syntax Description

none	Disables the delimiters (for example, xxxxxxxxxx).
colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).

Command Default

The default delimiter is hyphen.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aa:bb:cc:dd:ee:ff:

```
(Cisco Controller) > config macfilter mac-delimiter colon
```

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aa-bb-cc-dd-ee-ff:

```
(Cisco Controller) > config macfilter mac-delimiter hyphen
```

The following example shows how to have the operating system send MAC addresses to the RADIUS server in the form aabbccddeeff:

```
(Cisco Controller) > config macfilter mac-delimiter none
```

Related Commands

show macfilter

config macfilter radius-compat

To configure the Cisco wireless LAN controller for compatibility with selected RADIUS servers, use the **config macfilter radius-compat** command.

config macfilter radius-compat {**cisco** | **free** | **other**}

Syntax Description

cisco	Configures the Cisco ACS compatibility mode (password is the MAC address of the server).
free	Configures the Free RADIUS server compatibility mode (password is secret).
other	Configures for other server behaviors (no password is necessary).

Command Default

Other

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4.

The following example shows how to configure the Cisco ACS compatibility mode to “other”:

```
(Cisco Controller) > config macfilter radius-compat other
```

Related Commands

show macfilter

config macfilter wlan-id

To modify a wireless LAN ID for a MAC filter, use the **config macfilter wlan-id** command.

config macfilter wlan-id *MAC_addr WLAN_id*

Syntax Description

MAC addr	Client MAC address.
WLAN_id	Wireless LAN identifier to associate with. A value of zero is not allowed.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify client wireless LAN ID 2 for a MAC filter 11:11:11:11:11:11:

```
(Cisco Controller) > config macfilter wlan-id 11:11:11:11:11:11 2
```

Related Commands

show macfilter

show wlan

config mdns ap

To configure multicast Domain Name System (mDNS) snooping on an access point, use the **config mdns ap** command.

config mdns ap {**enable** {*ap_name* | **all**} [**vlan** *vlan_id*] | **disable** {*ap_name* | **all**} | **vlan** {**add** | **delete**} *vlan ap_name*}

Syntax Description

enable	Enables mDNS snooping on an access point.
ap_name	Name of the access point on which mDNS snooping has to be configured.
all	Configures mDNS snooping on all access points.
vlan	(Optional) Configures the VLAN on which the access point snoops and forwards the mDNS packets.
vlan_id	VLAN identifier.
disable	Disables mDNS snooping on an access point.
add	Adds a VLAN from which the access point snoops and forwards the mDNS packets to the controller. You can configure up to 10 VLANs for an mDNS access point.
delete	Deletes a VLAN from which the access point snoops and forwards the mDNS packets to the controller.

Command Default

The mDNS-enabled access point snoops the access or native VLANs by default.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

Enabling mDNS snooping on access points allows the access points to snoop the wired services on VLANs that are invisible to the controller. mDNS snooping is supported only on local-mode and monitor-mode access points. The access point must be in the access mode or trunk mode. If the access point is in the trunk mode, you must configure the VLAN on the controller on which the access point snoops and forwards the mDNS packets. You must also configure the native VLAN from the controller for the access point to snoop and send mDNS queries on. The access point also tags the packets with the native VLAN.

Global mDNS snooping overrides mDNS access point snooping.

The following example shows how to enable mDNS snooping on an access point and the VLAN on which it must snoop for mDNS packets:

```
(Cisco Controller) > config mdns ap enable vlan 1
```

config mdns profile

To configure a multicast DNS (mDNS) profile and associate a service with the profile, use the **config mdns profile** command.

config mdns profile {**create** | **delete** | **service** {**add** | **delete**} *service _name profile_name*

Syntax Description

create	Creates an mDNS profile.
delete	Deletes an mDNS profile. If the profile is associated to an interface group, an interface, or a WLAN, an error appears.
service	Configures an mDNS service.
add	Adds an mDNS service to an mDNS profile.
delete	Deletes an mDNS service from an mDNS profile.
service -name	Name of the mDNS service.
profile_name	Name of the mDNS profile. You can create a maximum of 16 profiles.

Command Default

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

After creating a new profile, you must map the profile to an interface group, an interface, or a WLAN. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

By default, the controller has an mDNS profile, default-mdns-profile. You cannot delete this default profile.

The following example shows how to add the Apple TV mDNS service to the mDNS profile1.

```
(Cisco Controller) > config mdns profile create profile1 Apple TV
```

Related Commands

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

To configure the query interval for multicast DNS (mDNS) services, use the **config mdns query interval** command.

config mdns query interval *interval_value*

Syntax Description

interval_value	mDNS query interval, in minutes, that you can set. The query interval is the frequency at which the controller sends periodic queries to all the services defined in the Master Services database. The range is from 10 to 120.

Command Default

The default query interval for an mDNS service is 15 minutes.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

The controller snoops and learns about the mDNS service advertisements only if the service is available in the Master Services database. mDNS uses the multicast IP address 224.0.0.251 as the destination address and 5353 as UDP destination port.

The following example shows how to configure the query interval for mDNS services as 20 minutes.

```
(Cisco Controller) > config mdns query interval 20
```

Related Commands

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

To configure multicast DNS (mDNS) services in the master services database, use the **config mdns service** command.

The following command is valid in Release 7.5 and later releases:

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**}}

Syntax Description

create	Adds a new mDNS service to the Master Services database.
service_name	Name of the mDNS service, for example, Air Tunes, iTunes Music Sharing, FTP, Apple File Sharing Protocol (AFP).
service_string	Unique string associated to an mDNS service, for example, _airplay._tcp.local. is the service string associated with Apple TV.
delete	Deletes an mDNS service from the Master Services database. Before deleting the service, the controller checks if any profile is using the service. **Note** You must delete the service from all profiles before deleting it.
query	Configures the query status for the mDNS service.
enable	Enables periodic query for an mDNS service by the controller.
disable	Disables periodic query for an mDNS service by the controller.
origin	Configures the origin of the mDNS service. You can restrict the origin of the service as wired or wireless.
Wireless	Configures the origin of the mDNS service as wireless.
Wired	Configures the origin of the mDNS service as wired.
All	Configures the origin of the mDNS service as wireless or wired.
lss	Configures Location Specific Services (LSS) for a service or all mDNS services. LSS is not applicable for registered service providers. The registered service providers are always included if the querying client corresponds to the user. You cannot configure LSS on the services configured as only wired.
all	Configures LSS for all mDNS services.
priority-mac	Configures the MAC address of a service provider device. This device gets a priority even if the service provider database is full.

add	Adds the MAC address of a service provider device for priority. You can configure up to 50 MAC addresses for a service.
delete	Deletes the MAC address of a service provider device from the priority list.
priority-mac	MAC address of a service provider device that needs priority. The MAC address must be unique for each service.
ap-group	Configures the access point group for wired service providers. These service providers get priority over others. When a client mNDS query originates from this AP group, the wired entries with priority MAC addresses and access point groups are listed first in the aggregated response.
ap-group-name	Name of the access point group to which the service provider belongs.

Command Default

By default, LSS is disabled, but it is enabled for all the discovered services.

Command History

Release	Modification
7.4	This command was introduced.
7.5	This command was modified. The **origin**, **Wireless**, **Wired**, **All**, **lss**, **priority-mac**, **add**, **delete**, **ap-group** keywords and *priority-mac ap-group-name* arguments were added.

Usage Guidelines

In Release 7.5 and later releases, the maximum number of service providers for different controller models are as follows:

- Cisco 5500 Series Controller and Cisco 2500 Series Controller—6400
- Cisco Wireless Services Module 2—6400
- Cisco 8500 Series Controller and Cisco 7500 Series Controller—16000

You cannot change the services with the origin set to Wireless to Wired if LSS is enabled for the service.

The following example shows how to add the HTTP mDNS service to the Master Services database, configure the origin as wireless, and enable LSS for the service:

```
(Cisco Controller) > config mdns service create http _http._tcp.local. origin wireless lss
 enable
```

The following example shows how to add a priority MAC address of a HTTP service provider device:

```
(Cisco Controller) >config mdns service priority-mac add 44:03:a7:a3:04:45 http
```

config mdns snooping

To enable or disable global multicast DNS (mDNS) snooping on the controller, use the **config mdns snooping** command.

config mdns snooping {**enable** | **disable**}

Syntax Description

enable	Enables mDNS snooping on the controller.
disable	Disables mDNS snooping on the controller.

Command Default

By default, mDNS snooping is enabled on the controller.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

mDNS service discovery provides a way to announce and discover services on the local network. mDNS perform DNS queries over IP multicast. mDNS supports zero configuration IP networking.

The following example shows how to enable mDNS snooping:

```
(Cisco Controller) > config mdns snooping enable
```

Related Commands

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

To configure the mDNS policy use the **config mdns policy enable | disable** command.

config mdnspolicyenable | disable

Syntax Description

policy	Name of the mDNS policy.
enable	Enables the policy for an mDNS service by the controller.
disable	Disables the policy for an mDNS service by the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

This command is valid for 8.0 release onwards.

Example

The following example show how to configure the mDNS policy.

```
(Cisco Controller) >config mdns
  policy enable
```

config mdns policy service-group

To create or delete mDNS policy service group use the **config mdns policy service-group** command.

config mdns policy service-group {**create** | **delete**} *service-group-name*

Syntax Description

create	Creates the mDNS service group.
delete	Deletes the mDNS service group.
service-group-name	Name of the service group.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example shows how to delete a mDNS service group.

```
(Cisco Controller) >config mdns policy service-group create <service-group-name>
```

config mdns policy service-group parameters

To configure the parameters of a service group, use the **config mdns policy service-group** command.

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]*

Syntax Description

device-mac	Configures MAC address of a service provider device.
add	Adds the service group name of the service provider device.
service-group-name	Name of a mDNS service group.
device-name	Name of a device to which the service provider belongs.
location type	Configures a location type of a service provider device.
[AP_LOCATION | AP_NAME | AP_GROUP]	Name, location, group of the access point.
device-location	Configures location of a device to which the service provider belongs.
[location string |any | same]	location string of a device.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example shows how to configure a location type of a service provider device.

```
(Cisco Controller) >config mdns policy service-group location type [AP_LOCATION | AP_NAME
| AP_GROUP]
```

config mdns policy service-group user-name

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-name add | delete <service-group-name> <user-role-name>**command

config mdnspolicyservice-groupuser-nameadd | delete*service-group-name user-name*

Syntax Description

user-name	Configures name of a user for mDNS service group.
service-group-name	Name of a mDNS service group
user-name	Name of the user role for mDNS service group

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example show how to add user name for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-name add <service-group-name>
<user-role-name>
```

config mdns policy service-group user-role

To configure a user role for a mDNS service group, use the **config mdns policy service-group user-role add | delete <service-group-name> <user-role-name>**command.

config mdnspolicyservice-groupuser-roleadd | delete*service-group-name user-role-name*

Syntax Description

user-role	Configures a user role for mDNS service group.
service-group-name	Name of a mDNS service group
user-role-name	Name of the user role for mDNS service group

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Example

The following example show how to add user role details for a mDNS service group

```
(Cisco Controller) >config mdns policy service-group user-role add <service-group-name>
<user-role-name>
```

config media-stream multicast-direct

To configure the media-stream multicast direct, use the **config media-stream multicast direct** command.

config media-stream multicast-direct {**enable** | **disable**}

Syntax Description

enable	Enables a media stream.
disable	Disables a media stream.

Command Default

None.

Usage Guidelines

Media-stream multicast-direct requires load based Call Admission Control (CAC) to run.

This example shows how to enable media-stream multicast-direct settings:

```
> config media-stream multicast-direct enable
```

This example shows how to disable media-stream multicast-direct settings:

```
> config media-stream multicast-direct disable
```

Related Commands

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

To configure various parameters of message configuration, use the **config media-stream message** command.

config media-stream message {**state** [**enable** | **disable**] | **url** *url* | **email** *email* | **phone** *phone_number* | **note** *note*}

Syntax Description

state	Specifies the media stream message state.
enable	(Optional) Enables the session announcement message state.
disable	(Optional) Disables the session announcement message state.
url	Configures the URL.
url	Session announcement URL.
email	Configures the email ID.
email	Specifies the session announcement e-mail.
phone	Configures the phone number.
phone_number	Session announcement phone number.
note	Configures the notes.
note	Session announcement notes.

Command Default

Disabled.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to enable the session announcement message state:

```
> config media-stream message state enable
```

This example shows how to configure the session announcement e-mail address:

```
> config media-stream message mail abc@co.com
```

Related Commands

config media-stream

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream add

To configure the various global media-stream configurations, use the **config media-stream add** command.

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**}

Syntax Description

multicast-direct	Specifies the media stream for the multicast-direct setting.
media_stream_name	Media-stream name.
start-IP	IP multicast destination start address.
end-IP	IP multicast destination end address.
template	(Optional) Configures the media stream from templates.
very coarse	Applies a very-coarse template.
coarse	Applies a coarse template.
ordinary	Applies an ordinary template.
low-resolution	Applies a low-resolution template.
med-resolution	Applies a medium-resolution template.
high-resolution	Applies a high-resolution template.
detail	Configures the media stream with specific parameters.
bandwidth	Maximum expected stream bandwidth.
packet-size	Average packet size.
periodic	Specifies the periodic admission evaluation.
initial	Specifies the Initial admission evaluation.
qos	AIR QoS class (video only).
priority	Media-stream priority.
drop	Specifies that the stream is dropped on a periodic reevaluation.
fallback	Specifies if the stream is demoted to the best-effort class on a periodic reevaluation.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to configure a new media stream:

```
> config media-stream add multicast-direct abc 227.8.8.8 227.9.9.9 detail 2 150 periodic
video 1 drop
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream admit

To allow traffic for a media stream group, use the **config media-stream admit** command.

config media-stream admit *media_stream_name*

Syntax Description

media_stream_name	Media-stream group name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you try to allow traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.

This example shows how to allow traffic for a media stream group:

```
(Cisco Controller) > config media-stream admit MymediaStream
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream deny

To block traffic for a media stream group, use the **config media-stream deny** command.

Syntax Description

media_stream_name	Media-stream group name.

config media-stream deny *media_stream_name*

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you try to block traffic for the media stream group, you will be prompted that IGMP snooping will be disabled and enabled again, and all clients might observe a glitch on the multicast traffic.

This example shows how to block traffic for a media stream group:

```
(Cisco Controller) > config media-stream deny MymediaStream
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config media-stream delete

To configure the various global media-stream configurations, use the **config media-stream delete** command.

config media-stream delete *media_stream_name*

Syntax Description

media_stream_name	Media-stream name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Media-stream multicast-direct requires load-based Call Admission Control (CAC) to run.

This example shows how to delete the media stream named abc:

```
(Cisco Controller) > config media-stream delete abc
```

Related Commands

show 802.11a media-stream name

show media-stream group summary

show media-stream group detail

config memory monitor errors

To enable or disable monitoring for memory errors and leaks, use the **config memory monitor errors** command.

config memory monitor errors {**enable** | **disable**}

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

enable	Enables the monitoring for memory settings.
disable	Disables the monitoring for memory settings.

Command Default

Monitoring for memory errors and leaks is disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

The following example shows how to enable monitoring for memory errors and leaks for a controller:

```
(Cisco Controller) > config memory monitor errors enable
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config memory monitor leaks

To configure the controller to perform an auto-leak analysis between two memory thresholds, use the **config memory monitor leaks** command.

config memory monitor leaks *low_thresh high_thresh*

Caution The **config memory monitor** commands can be disruptive to your system and should be run only when you are advised to do so by the Cisco TAC.

Syntax Description

low_thresh	Value below which free memory cannot fall without crashing. This value cannot be set lower than 10000 KB.
high_thresh	Value below which the controller enters auto-leak-analysis mode. See the "Usage Guidelines" section.

Command Default

The default value for *low_thresh* is 10000 KB; the default value for *high_thresh* is 30000 KB.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Note Be cautious about changing the defaults for the **config memory monitor** command unless you know what you are doing, you have detected a problem, or you are collecting troubleshooting information.

Use this command if you suspect that a memory leak has occurred.

If the free memory is lower than the *low_thresh* threshold, the system crashes, generating a crash file. The default value for this parameter is 10000 KB, and you cannot set it below this value.

Set the *high_thresh* threshold to the current free memory level or higher so that the system enters auto-leak-analysis mode. After the free memory reaches a level lower than the specified *high_thresh* threshold, the process of tracking and freeing memory allocation begins. As a result, the **debug memory events enable** command shows all allocations and frees, and the **show memory monitor detail** command starts to detect any suspected memory leaks.

The following example shows how to set the threshold values for auto-leak-analysis mode to 12000 KB for the low threshold and 35000 KB for the high threshold:

```
(Cisco Controller) > config memory monitor leaks 12000 35000
```

Related Commands

config memory monitor leaks

debug memory

show memory monitor

config mesh alarm

To configure alarm settings for outdoor mesh access points, use the **config mesh alarm** command.

config mesh alarm {**max-hop** | **max-children** | **low-snr** | **high-snr** | **association** | **parent-change count**} *value*

Syntax Description

max-hop	Sets the maximum number of hops before triggering an alarm for traffic over the mesh network. The valid values are 1 to 16 (inclusive).
max-children	Sets the maximum number of mesh access points (MAPs) that can be assigned to a mesh router access point (RAP) before triggering an alarm. The valid values are 1to 16 (inclusive).
low-snr	Sets the low-end signal-to-noise ratio (SNR) value before triggering an alarm. The valid values are 1 to 30 (inclusive).
high-snr	Sets the high-end SNR value before triggering an alarm. The valid values are 1 to 30 (inclusive).
association	Sets the mesh alarm association count value before triggering an alarm. The valid values are 1 to 30 (inclusive).
parent-change count	Sets the number of times a MAP can change its RAP association before triggering an alarm. The valid values are 1 to 30 (inclusive).
value	Value above or below which an alarm is generated. The valid values vary for each command.

Command Default

See the "Syntax Description" section for command and argument value ranges.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the maximum hops threshold to 8:

```
(Cisco Controller) >config mesh alarm max-hop 8
```

The following example shows how to set the upper SNR threshold to 25:

```
(Cisco Controller) >config mesh alarm high-snr 25
```

config mesh astools

To globally enable or disable the anti-stranding feature for outdoor mesh access points, use the **config mesh astools** command.

config mesh astools {**enable** | **disable**}

Syntax Description

enable	Enables this feature for all outdoor mesh access points.
disable	Disables this feature for all outdoor mesh access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable anti-stranding on all outdoor mesh access points:

```
(Cisco Controller) >config mesh astools enable
```

config mesh backhaul rate-adapt

To globally configure the backhaul Tx rate adaptation (universal access) settings for indoor and outdoor mesh access points, use the **config mesh backhaul rate-adapt** command.

config mesh backhaul rate-adapt [**all** | **bronze** | **silver** | **gold** | **platinum**] {**enable** | **disable**}

Syntax Description

all	(Optional) Grants universal access privileges on mesh access points.
bronze	(Optional) Grants background-level client access privileges on mesh access points.
silver	(Optional) Grants best effort-level client access privileges on mesh access points.
gold	(Optional) Grants video-level client access privileges on mesh access points.
platinum	(Optional) Grants voice-level client access privileges on mesh access points.
enable	Enables this backhaul access level for mesh access points.
disable	Disables this backhaul access level for mesh access points.

Command Default

Backhaul access level for mesh access points is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To use this command, mesh backhaul with client access must be enabled by using the **config mesh client-access** command.

Note After this feature is enabled, all mesh access points reboot.

The following example shows how to set the backhaul client access to the best-effort level:

```
(Cisco Controller) >config mesh backhaul rate-adapt silver
```

config mesh backhaul slot

To configure the slot radio as a downlink backhaul, use the **config mesh backhaul slot** command.

config mesh backhaul slot *slot_id* {**enable** | **disable**} *cisco_ap*

Syntax Description

slot_id	Slot number between 0 and 2.
enable	Enables the entered slot radio as a downlink backhaul.
disable	Disables the entered slot radio as a downlink backhaul.
cisco_ap	Name of the Root AP of the sector on which the backhaul needs to be enabled or disabled.

Command Default

The entered slot radio as a downlink backhaul is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For 2.4 GHz, only slot 0 and 1 are valid. If slot 0 is enabled, slot 1 is automatically be disabled. If slot 0 is disabled, slot 1 is automatically enabled.

The following example shows how to enable slot 1 as the preferred backhaul for the root AP myrootap1:

```
(Cisco Controller) >config mesh backhaul slot 1 enable myrootap1
```

config mesh battery-state

To configure the battery state for Cisco mesh access points, use the **config mesh battery-state** command.

config mesh battery-state disable {**all** | *cisco_ap*}

Syntax Description

disable	Disables the battery-state for mesh access points.
all	Applies this command to all mesh access points.
cisco_ap	Specific mesh access point.

Command Default

Battery state is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable battery state for all mesh APs:

```
(Cisco Controller) >config mesh battery-state disable all
```

config mesh client-access

To enable or disable client access to the mesh backhaul on indoor and outdoor mesh access points, use the **config mesh client-access** command.

config mesh client-access {**enable** [**extended**] | **disable**}

Syntax Description

enable	Allows wireless client association over the mesh access point backhaul 802.11a radio.
extended	(Optional) Enables client access over both the backhaul radios for backhaul access points.
disable	Restricts the 802.11a radio to backhaul traffic, and allows client association only over the 802.11b/g radio.

Command Default

Client access is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Backhaul interfaces (802.11a radios) act as primary Ethernet interfaces. Backhauls function as trunks in the network and carry all VLAN traffic between the wireless and wired network. No configuration of primary Ethernet interfaces is required.

When this feature is enabled, the mesh access points allow wireless client association over the 802.11a radio, which implies that a 152x mesh access point can carry both backhaul traffic and 802.11a client traffic over the same 802.11a radio.

When this feature is disabled, the mesh access points carry backhaul traffic over the 802.11a radio and allows client association only over the 802.11b/g radio.

The following example shows how to enable client access extended to allow a wireless client association over the 802.11a radio:

```
(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
```

The following example shows how to restrict a wireless client association to the 802.11b/g radio:

```
(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 ethernet-bridging allow-bpdu

To configure STP BPDUs towards wired mesh uplink, use the **config mesh ethernet-bridging allow-bpdu** command.

config mesh ethernet-bridging allow-bpdu {**enable** | **disable**}

Syntax Description

enable	Enables STP BPDUs towards wired mesh uplink.
disable	Disables STP BPDUs towards wired mesh uplink.

Command Default

Disabled

Command History

Release	Modification
8.0.110.0	This command was introduced.

Usage Guidelines

controller does not allow you to use this command if VLAN transparency is enabled.

config mesh ethernet-bridging vlan-transparent

To configure how a mesh access point handles VLAN tags for Ethernet bridged traffic, use the **config mesh ethernet-bridging vlan-transparent** command.

config mesh ethernet-bridging vlan-transparent {**enable** | **disable**}

Syntax Description

enable	Bridges packets as if they are untagged.
disable	Drops all tagged packets.

Command Default

Bridges packets as if they are untagged.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure Ethernet packets as untagged:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent enable
```

The following example shows how to drop tagged Ethernet packets:

```
(Cisco Controller) >config mesh ethernet-bridging vlan-transparent disable
```

config mesh full-sector-dfs

To globally enable or disable full-sector Dynamic Frequency Selection (DFS) on mesh access points, use the **config mesh full-sector-dfs** command.

config mesh full-sector-dfs {**enable** | **disable**}

Syntax Description

enable	Enables DFS for mesh access points.
disable	Disables DFS for mesh access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command instructs the mesh sector to make a coordinated channel change on the detection of a radar signal. For example, if a mesh access point (MAP) detects a radar signal, the MAP will notify the root access point (RAP), and the RAP will initiate a sector change.

All MAPs and the RAP that belong to that sector go to a new channel, which lowers the probability of MAPs stranding when radar is detected on the current backhaul channel, and no other valid parent is available as backup.

Each sector change causes the network to be silent for 60 seconds (as dictated by the DFS standard).

It is expected that after a half hour, the RAP will go back to the previously configured channel, which means that if radar is frequently observed on a RAP's channel, it is important that you configure a different channel for that RAP to exclude the radar affected channel at the controller.

This example shows to enable full-sector DFS on mesh access points:

```
(Cisco Controller) >config mesh full-sector-dfs enable
```

config mesh linkdata

To enable external MAC filtering of access points, use the **config mesh linkdata** command.

config mesh linkdata *destination_ap_name*

Syntax Description

destination_ap_name	Destination access point name for MAC address filtering.

Command Default

External MAC filtering is disabled.

Usage Guidelines

Note The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first execute the **config mesh linktest** command with the access point that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display the link data will display (see example).

MAC filtering uses the local MAC filter on the controller by default.

When external MAC filter authorization is enabled, if the MAC address is not found in the local MAC filter, then the MAC address in the external RADIUS server is used.

MAC filtering protects your network against rogue mesh access points by preventing access points that are not defined on the external server from joining.

Before employing external authentication within the mesh network, the following configuration is required:

- The RADUIS server to be used as an AAA server must be configured on the controller.
- The controller must also be configured on the RADIUS server.
- The mesh access point configured for external authorization and authentication must be added to the user list of the RADIUS server.

The following example shows how to enable external MAC address filtering on access point AP001d.710d.e300:

```
(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%
```

This example shows how to enable external MAC filtering on access point AP001d.71d.e300:

```
(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

To verify client access between mesh access points, use the **config mesh linktest** command.

config mesh linktest *source_ap* {*dest_ap* | *MAC addr*} *datarate packet_rate packet_size duration*

Syntax Description

source_ap	Source access point.
dest_ap	Destination access point.
MAC addr	MAC address.
datarate	• Data rate for 802.11a radios. Valid values are 6, 9, 11, 12, 18, 24, 36, 48 and 54 Mbps. • Data rate for 802.11b radios. Valid values are 6, 12, 18, 24, 36, 54, or 100 Mbps. • Data rate for 802.11n radios. Valid values are MCS rates between m0 to m15.
packet_rate	Number of packets per second. Valid range is 1 through 3000, but the recommended default is 100.
packet_size	(Optional) Packet size in bytes. If not specified, packet size defaults to 1500 bytes.
duration	(Optional) Duration of the test in seconds. Valid values are 10-300 seconds, inclusive. If not specified, duration defaults to 30 seconds.

Command Default

100 packets per second, 1500 bytes, 30-second duration.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The **config mesh linktest** and **config mesh linkdata** commands are designed to be used together to verify information between a source and a destination access point. To get this information, first enter the **config mesh linktest** command with the access point that you want link data from in the *dest_ap* argument. When the command completes, enter the **config mesh linkdata** command and list the same destination access point, to display the link data.

The following warning message appears when you run a linktest that might oversubscribe the link:

```
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?
```

The following example shows how to verify client access between mesh access points *SB_MAP1* and *SB_RAP2* at *36 Mbps*, *20 fps*, *100 frame size*, and *15*-second duration:

```
(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%
```

The following table lists the output flags displayed for the **config mesh linktest** command.

Table 6: Output Flags for the Config Mesh Linktest Command

Output Flag	Description
txPkts	Number of packets sent by the source.
txBuffAllocErr	Number of linktest buffer allocation errors at the source (expected to be zero).
txQFullErrs	Number of linktest queue full errors at the source (expected to be zero).
Total rx pkts heard at destination	Number of linktest packets received at the destination (expected to be same as or close to the txPkts).

Output Flag	Description
rx pkts decoded correctly	Number of linktest packets received and decoded correctly at the destination (expected to be same as close to txPkts).
err pkts: Total	Packet error statistics for linktest packets with errors.
rx lost packets	Total number of linktest packets not received at the destination.
rx dup pkts	Total number of duplicate linktest packets received at the destination.
rx out of order	Total number of linktest packets received out of order at the destination.
avgNF	Average noise floor.
Noise Floor profile	Noise floor profile in dB and are negative numbers.
avgSNR	Average SNR values.
SNR profile [odb...60dB]	Histogram samples received between 0 to 60 dB. The different colums in the SNR profile is the number of packets falling under the bucket 0-3, 3-6, 6-9, up to 57-60.
avgRSSI	Average RSSI values. The average high and low RSSI values are positive numbers.
RSSI profile [-100dB...-40dB]	The RSSI profile in dB and are negative numbers.

config mesh lsc

To configure a locally significant certificate (LSC) on mesh access points, use the **config mesh lsc** command.

config mesh lsc {**enable** | **disable**}

Syntax Description

enable	Enables an LSC on mesh access points.
disable	Disables an LSC on mesh access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable LSC on mesh access points:

```
(Cisco Controller) >config mesh lsc enable
```

config mesh lsc advanced

To configure an advanced locally significant certificate (LSC) when a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh Access Point (AP), use the **config mesh lsc advanced** command.

config mesh lsc advanced {**enable** | **disable**}

Syntax Description

enable	Enables advanced LSC for a mesh AP.
disable	Disables advanced LSC for a mesh AP.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable advanced LSC for a mesh AP:

```
(Cisco Controller) >config  mesh lsc advanced enable
```

config mesh lsc advanced ap-provision

To configure advanced mesh locally significant certificate (LSC) Access Point (AP) provision if a wildcard is used in an external authentication, authorization, and accounting (AAA) server for a mesh AP, use the **config mesh lsc advanced ap-provision** command.

config mesh lsc advanced ap-provision {**enable** | **disable** | **open-window** {**enable** | **disable**} | **provision-controller** {**enable** | **disable**}}

Syntax Description

enable	Enables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP.
disable	Disables advanced mesh LSC AP provision if a wildcard is used in an external AAA server for a mesh AP .
open-window	Configures mesh LSC provision for all mesh APs without MAC validation.
enable	Enables AP provision for all mesh APs without MAC validation.
disable	Disables AP provision for all mesh APs without MAC validation.
provision-controller	Configures the provision controller details for mesh APs to get an LSC.
enable	Enables the provision controller option to get an LSC.
disable	Disables the provision controller option to get an LSC.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable the advanced AP provision method:

```
(Cisco Controller) >config mesh lsc advanced ap-provision enable
```

config mesh multicast

To configure multicast mode settings to manage multicast transmissions within the mesh network, use the **config mesh multicast** command.

config mesh multicast {**regular** | **in** | **in-out**}

Syntax Description

regular	Multicasts the video across the entire mesh network and all its segments by bridging-enabled root access points (RAPs) and mesh access points (MAPs).
in	Forwards the multicast video received from the Ethernet by a MAP to the RAP's Ethernet network. No additional forwarding occurs, which ensures that non-LWAPP multicasts received by the RAP are not sent back to the MAP Ethernet networks within the mesh network (their point of origin), and MAP-to-MAP multicasts do not occur because they are filtered out
in-out	Configures the RAP and MAP to multicast, but each in a different manner: If multicast packets are received at a MAP over Ethernet, they are sent to the RAP; however, they are not sent to other MAP Ethernets, and the MAP-to-MAP packets are filtered out of the multicast. If multicast packets are received at a RAP over Ethernet, they are sent to all the MAPs and their respective Ethernet networks. See the Usage Guidelines section for more information.

Command Default

In-out mode

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Multicast for mesh networks cannot be enabled using the controller GUI.

Mesh multicast modes determine how bridging-enabled access points mesh access points (MAPs) and root access points (RAPs) send multicasts among Ethernet LANs within a mesh network. Mesh multicast modes manage non-LWAPP multicast traffic only. LWAPP multicast traffic is governed by a different mechanism.

You can use the controller CLI to configure three mesh multicast modes to manage video camera broadcasts on all mesh access points. When enabled, these modes reduce unnecessary multicast transmissions within the mesh network and conserve backhaul bandwidth.

When using in-out mode, it is important to properly partition your network to ensure that a multicast sent by one RAP is not received by another RAP on the same Ethernet segment and then sent back into the network.

Note If 802.11b clients need to receive CAPWAP multicasts, then multicast must be enabled globally on the controller as well as on the mesh network (by using the **config network multicast global** command). If multicast does not need to extend to 802.11b clients beyond the mesh network, you should disable the global multicast parameter.

The following example shows how to multicast video across the entire mesh network and all its segments by bridging-enabled RAPs and MAPs:

```
(Cisco Controller) >config mesh multicast regular
```

config mesh parent preferred

To configure a preferred parent for a mesh access point, use the **config mesh parent preferred** command.

config mesh parent preferred *cisco_ap* {*mac_address* | **none**}

Syntax Description

cisco_ap	Name of the child access point.
mac_address	MAC address of the preferred parent.
none	Clears the configured parent.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A child AP selects the preferred parent based on the following conditions:

- The preferred parent is the best parent.
- The preferred parent has a link SNR of at least 20 dB (other parents, however good, are ignored).
- The preferred parent has a link SNR in the range of 12 dB and 20 dB, but no other parent is significantly better (that is, the SNR is more than 20 percent better). For an SNR lower than 12 dB, the configuration is ignored.
- The preferred parent is not in a blocked list.
- The preferred parent is not in silent mode because of dynamic frequency selection (DFS).
- The preferred parent is in the same bridge group name (BGN). If the configured preferred parent is not in the same BGN and no other parent is available, the child joins the parent AP using the default BGN.

The following example shows how to configure a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60
```

The following example shows how to clear a preferred parent with the MAC address 00:21:1b:ea:36:60 for a mesh access point myap1, by using the keyword none:

```
(Cisco Controller) >config mesh parent preferred myap1 00:21:1b:ea:36:60 none
```

config mesh public-safety

To enable or disable the 4.9-GHz public safety band for mesh access points, use the **config mesh public-safety** command.

config mesh public-safety {**enable** | **disable**} {**all** | *cisco_ap*}

Syntax Description

enable	Enables the 4.9-GHz public safety band.
disable	Disables the 4.9-GHz public safety band.
all	Applies the command to all mesh access points.
cisco_ap	Specific mesh access point.

Command Default

The 4.9-GHz public safety band is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

4.9 GHz is a licensed frequency band restricted to public-safety personnel.

The following example shows how to enable the 4.9-GHz public safety band for all mesh access points:

```
(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

To enable or disable external authentication for mesh access points, use the **config mesh radius-server** command.

config mesh radius-server *index* {**enable** | **disable**}

Syntax Description

index	RADIUS authentication method. Options are as follows: • Enter **eap** to designate Extensible Authentication Protocol (EAP) for the mesh RADIUS server setting. • Enter **psk** to designate Preshared Keys (PSKs) for the mesh RADIUS server setting.
enable	Enables the external authentication for mesh access points.
disable	Disables the external authentication for mesh access points.

Command Default

EAP is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable external authentication for mesh access points:

```
(Cisco Controller) >config mesh radius-server eap enable
```

config mesh range

To globally set the maximum range between outdoor root access points (RAPs) and mesh access points (MAPs), use the **config mesh range** command.

config mesh range [*distance*]

Syntax Description

distance	(Optional) Maximum operating range (150 to 132000 ft) of the mesh access point.

Command Default

12,000 feet.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

After this command is enabled, all outdoor mesh access points reboot. This command does not affect indoor access points.

The following example shows how to set the range between an outdoor mesh RAP and a MAP:

```
(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

To configure a secondary backhaul on the mesh network, use the **config mesh secondary-backhaul** command.

config mesh secondary-backhaul {**enable** [**force-same-secondary-channel**] | **disable** [**rll-retransmit** | **rll-transmit**]}

Syntax Description

enable	Enables the secondary backhaul configuration.
force-same-secondary-channel	(Optional) Enables secondary-backhaul mesh capability. Forces all access points rooted at the first hop node to have the same secondary channel and ignores the automatic or manual channel assignments for the mesh access points (MAPs) at the second hop and beyond.
disable	Specifies the secondary backhaul configuration is disabled.
rll-transmit	(Optional) Uses reliable link layer (RLL) at the second hop and beyond.
rll-retransmit	(Optional) Extends the number of RLL retry attempts in an effort to improve reliability.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command uses a secondary backhaul radio as a temporary path for traffic that cannot be sent on the primary backhaul due to intermittent interference.

The following example shows ho to enable a secondary backhaul radio and force all access points rooted at the first hop node to have the same secondary channel:

```
(Cisco Controller) >config mesh secondary-backhaul enable force-same-secondary-channel
```

config mesh security

To configure the security settings for mesh networks, use the **config mesh security** command.

config mesh security {{**rad-mac-filter** | **force-ext-auth** } {**enable** | **disable**}} | {{**eap** | **psk provisioning** | **provisioning window**} | {**enable** | **disable**}} | {**delete_psk** | **key**}

Syntax Description

rad-mac-filter	Enables a Remote Authentication Dial-In User Service (RADIUS) MAC address filter for the mesh security setting.
force-ext-auth	Disables forced external authentication for the mesh security setting.
lsc-only-auth	Enables Locally Significant Certificate only authentication for the mesh security setting.
enable	Enables the mesh security setting.
disable	Disables the mesh security setting.
eap	Designates the Extensible Authentication Protocol (EAP) for the mesh security setting by default.
psk	Designates a preshared key(PSK) for the mesh security setting.
provisioning	Encrypts provisioning for the PSK in the controller.
provisioning window	Encrypts provisioning window for the PSK in controller.
enable	Enables provisioning of the PSK.
disable	Disables provisioning of the PSK.
key	Specifies the key for the PSK.

Command Default

The EAP is designated as default for the mesh security.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2	This command was modified, the psk provisioning and psk provisioning keywords are added.

The following example shows how to configure EAP as the security option for all mesh access points:

```
(Cisco Controller) config mesh security eap
```

The following example shows how to configure PSK as the security option for all mesh access points:

```
(Cisco Controller) config mesh security psk
```

The following example shows how to enable PSK provisioning as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning enable
```

The following example shows how to configure a PSK provisioning key as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning key 5
```

The following example shows how to enable a PSK provisioning window as the security option for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning window enable
```

The following example shows how to delete the PSK provisioning for controller :

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc
```

The following example shows how to delete the PSK provisioning for all mesh access points:

```
(Cisco Controller)> config mesh security psk provisioning delete_psk ap
```

The following example shows how to delete PSK provisioning for all configurations in controller :

```
(Cisco Controller)> config mesh security psk provisioning delete_psk wlc all
```

config mesh slot-bias

To enable or disable slot bias for serial backhaul mesh access points, use the **config mesh slot-bias** command.

config mesh slot-bias {**enable** | **disable**}

Syntax Description

enable	Enables slot bias for serial backhaul mesh APs.
disable	Disables slot bias for serial backhaul mesh APs.

Command Default

By default, slot bias is in enabled state.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Follow these guidelines when using this command:

- The **config mesh slot-bias** command is a global command and therefore applicable to all 1524SB APs associated with the same controller.
- Slot bias is applicable only when both slot 1 and slot 2 are available. If a slot radio does not have a channel that is available because of dynamic frequency selection (DFS), the other slot takes up both the uplink and downlink roles.
- If slot 2 is not available because of hardware issues, slot bias functions normally. Corrective action should be taken by disabling the slot bias or fixing the antenna.

The following example shows how to disable slot bias for serial backhaul mesh APs:

```
(Cisco Controller) >config mesh slot-bias disable
```

config mgmtuser add

To add a local management user to the controller, use the **config mgmtuser add** command.

config mgmtuser add *username password* {**lobby-admin** | **read-write** | **read-only**} [*description*]

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
password	Account password. The password can be up to 24 alphanumeric characters.
lobby-admin	Creates a management user with lobby ambassador privileges.
read-write	Creates a management user with read-write access.
read-only	Creates a management user with read-only access.
description	(Optional) Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.4	This command creates lobby-admin user .

The following example shows how to create a management user account with read-write access.

```
(Cisco Controller) > config mgmtuser add admin admin read-write "Main account"
```

Related Commands

show mgmtuser

config mgmtuser delete

To delete a management user from the controller, use the **config mgmtuser delete** command.

config mgmtuser delete *username*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.

Command Default

The management user is not deleted by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a management user account admin from the controller.

```
(Cisco Controller) > config mgmtuser delete admin
Deleted user admin
```

Related Commands

show mgmtuser

config mgmtuser description

To add a description to an existing management user login to the controller, use the **config mgmtuser description** command.

config mgmtuser description *username description*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
description	Description of the account. The description can be up to 32 alphanumeric characters within double quotes.

Command Default

No description is added to the management user.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a description “primary-user” to the management user “admin”:

```
(Cisco Controller) > config mgmtuser description admin "primary-user"
```

Related Commands

config mgmtuser add

config mgmtuser delete

config mgmtuser password

show mgmtuser

config mgmtuser password

To configure a management user password, use the **config mgmtuser password** command.

config mgmtuser password *username password*

Syntax Description

username	Account username. The username can be up to 24 alphanumeric characters.
password	Account password. The password can be up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to change the password of the management user “admin” with the new password 5rTfm:

```
(Cisco Controller) > config mgmtuser password admin 5rTfm
```

Related Commands

show mgmtuser

config mgmtuser telnet

To enable local management users to use Telnet to connect to the controller, use the **config mgmtuser telnet** command.

config mgmtuser telnet *user_name* { **enable** | **disable** }

Syntax Description

user_name	Username of a local management user.
enable	Enables a local management user to use Telnet to connect to the controller. You can enter up to 24 alphanumeric characters.
disable	Disables a local management user from using Telnet to connect to the controller.

Command Default

Local management users can use Telnet to connect to the controller.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You must enable global Telnet to enable this command. Secure Shell (SSH) connection is not affected when you enable this option.

The following example shows how to enable a local management user to use Telnet to connect to the controller:

```
(Cisco Controller) > config mgmtuser telnet admin1 enable
```

config mgmtuser termination-interval

To configure the user re-authentication terminal interval in seconds, use the **config mgmtuser termination-interval** command.

config mgmtuser termination-interval {*seconds* }

Syntax Description

seconds	Re-authentication terminal interval in seconds for a user before being logged out. Default value is 0, the valid range is 0 to 300 seconds.

Command History

Release	Modification
8.2	This command was introduced in this release.

The following example shows how to set the interval in seconds before the user is logged out:

```
(Cisco Controller) > config mgmtuser termination-interval 180
```

config mobility dscp

To configure the mobility intercontroller DSCP value, use the **config mobility dscp** command.

config mobility dscp *dscp_value*

Syntax Description

dscp_value	DSCP value ranging from 0 to 63.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the mobility intercontroller DSCP value to 40:

```
(Cisco Controller) >config mobility dscp 40
```

config mobility encryption tunnel

To configure the mobility encryption tunnel on a controller, use the **config mobility encryption** command.

config mobility encryption { **enable | disable** }

Syntax Description

enable	Enables mobility encrypt tunnel on a controller.
disable	Disables mobility encrypt tunnel on a controller.

Command Default

None

Command History

Release	Modification
8.7	This command was introduced.

The following example shows how to enable mobility encrypt tunnel on a controller:

```
(Cisco Controller) >config mobility encrypt tunnel enable
```

config mobility group anchor

To create a new mobility anchor for the WLAN or wired guest LAN, enter, use the **config mobility group anchor** command.

config mobility group anchor {**add** | **delete**} {**wlan** *wlan_id* | **guest-lan** *guest_lan_id*} *anchor_ip*

Syntax Description

add	Adds or changes a mobility anchor to a wireless LAN.
delete	Deletes a mobility anchor from a wireless LAN.
wlan	Specifies the wireless LAN anchor settings.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).
guest-lan	Specifies the guest LAN anchor settings.
guest_lan_id	Guest LAN identifier between 1 and 5 (inclusive).
anchor_ip	IP address of the anchor controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The *wlan_id* or *guest_lan_id* must exist and be disabled.

Auto-anchor mobility is enabled for the WLAN or wired guest LAN when you configure the first mobility anchor. Deleting the last anchor disables the auto-anchor mobility feature and resumes normal mobility for new associations.

The following example shows how to add a mobility anchor with the IP address 192.12.1.5 to a wireless LAN ID 2:

```
(Cisco Controller) >config mobility group anchor add wlan 2 192.12.1.5
```

The following example shows how to delete a mobility anchor with the IP address 193.13.1.15 from a wireless LAN:

```
(Cisco Controller) >config mobility group anchor delete wlan 5 193.13.1.5
```

config mobility group domain

To configure the mobility domain name, use the **config mobility group domain** command.

config mobility group domain *domain_name*

Syntax Description

domain_name	Domain name. The domain name can be up to 31 case-sensitive characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a mobility domain name lab1:

```
(Cisco Controller) >config mobility group domain lab1
```

config mobility group keepalive count

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive count** command.

config mobility group keepalive count *count*

Syntax Description

count	Number of times that a ping request is sent to a mobility group member before the member is considered unreachable. The range is from 3 to 20. The default is 3.

Command Default

The default number of times that a ping request is sent to a mobility group member is 3.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the number of times a ping request is sent to a mobility group member before the member is considered unreachable to three counts:

```
(Cisco Controller) >config mobility group keepalive count 3
```

config mobility group keepalive interval

To configure the controller to detect failed mobility group members (including anchor controllers), use the **config mobility group keepalive** command.

config mobility group keepalive *interval*

Syntax Description

interval	Interval of time between each ping request sent to a mobility group member. The range is from 1 to 30 seconds. The default value is 10 seconds.

Command Default

The default interval of time between each ping request is 10 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
(Cisco Controller) >config mobility group keepalive 10
```

config mobility group member

To add or delete users from the mobility group member list, use the **config mobility group member** command.

config mobility group member {**add** *MAC-addr IP-addr* [*group_name*] [**encrypt**{**enable** | **disable**] | [**data-dtls** *mac-addr* {**enable** | **disable**} | **delete** *MAC-addr* | **hash** *IP-addr* {*key* | **none**}}

Syntax Description

add	Adds or changes a mobility group member to the list.
MAC-addr	Member switch MAC address.
IP-addr	Member switch IP address.
group_name	(Optional) Member switch group name (if different from the default group name).
delete	(Optional) Deletes a mobility group member from the list.
hash	Configures the hash key for authorization. You can configure the hash key only if the member is a virtual controller in the same domain.
key	Hash key of the virtual controller. For example, a819d479dcfeb3e0974421b6e8335582263d9169
none	Clears the previous hash key of the virtual controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.
8.8.111.0	This command was updated by adding **encrypt** , **data-dtls** keywords to support IRCM functionality.

The following example shows how to add a mobility group member with an IPv4 address to the list:

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 209.165.200.225
```

The following example shows how to add a mobility group member with an IPv6 address to the list:

```
(Cisco Controller) >config mobility group member add 11:11:11:11:11:11 2001:DB8::1
```

The following example shows how to configure the hash key of a virtual controller in the same domain:

Note The IP address in this example can be in either IPv4 or IPv6 format.

```
(Cisco Controller) >config mobility group member hash 209.165.201.1
a819d479dcfeb3e0974421b6e8335582263d9169
```

config mobility group multicast-address

To configure the multicast group IP address for nonlocal groups within the mobility list, use the **config mobility group multicast-address** command.

config mobility group multicast-address *group_name ip_address*

Syntax Description

group_name	Member switch group name (if different from the default group name).
ip_address	Member switch IP address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the multicast group IP address 10.10.10.1 for a group named test:

```
(Cisco Controller) >config mobility group multicast-address test 10.10.10.1
```

The following example shows how to configure the multicast group IP address 2001:DB8::1 for a group named test:

```
(Cisco Controller) >config mobility group multicast-address test 2001:DB8::1
```

config mobility multicast-mode

To enable or disable mobility multicast mode, use the **config mobility multicast-mode** command.

config mobility multicast-mode {**enable** | **disable**} *local_group_multicast_address*

Syntax Description

enable	Enables the multicast mode; the controller u to send Mobile Announce messages to the lo
disable	Disables the multicast mode; the controller u send the Mobile Announce messages to the
local_group_multicast_address	IP address for the local mobility group.

Command Default

The mobility multicast mode is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the multicast mobility mode for the local mobility group IP address 157.168.20.0:

```
(Cisco Controller) >config mobility multicast-mode enable 157.168.20.0
```

config mobility new-architecture

To enable new mobility on the controller, use the **config mobility new-architecture** command.

config mobility new-architecture {**enable** | **disable**}

Syntax Description

enable	Configures the controller to switch to the new mobility architecture.
disable	Configures the controller to switch to the old flat mobility architecture.

Command Default

By default, new mobility is disabled.

Command History

Release	Modification
7.3.112.0	This command was introduced.

Usage Guidelines

New mobility is supported only on Cisco WiSM2, Cisco 2500 Series Wireless Controllers, Cisco 5500 Series Wireless Controllers, and Cisco 8500 Series Wireless Controllers. New mobility enables the controller to be compatible with Converged Access controllers with Wireless Control Module (WCM), such as Cisco Catalyst 3850 Series and the Cisco 5760 Wireless LAN Controllers.

The following example shows how to enable new mobility on the controller:

```
(Cisco Controller) >config mobility new-architecture enable
```

config mobility oracle

To configure the Mobility Oracle (MO), use the **config mobility oracle** command.

config mobility oracle {**enable** | **disable** | **ip** *ip_address*}

Syntax Description

enable	Enables the MO on startup.
disable	Disables the MO on startup.
ip	Specifies the IP address of the MO.
ip_address	IP address of the MO.

Command Default

None

Command History

Release	Modification
7.3.112.0	This command was introduced.
8.0	This command supports only IPv4 address format.

Usage Guidelines

The MO maintains the client database under one complete mobility domain. It consists of a station database, an interface to the mobility controller, and an NTP server. There can be only one MO in the entire mobility domain.

The IPv6 address format for this command is not supported.

The following example shows how to configure the MO IP address:

```
(Cisco Controller) >config mobility oracle ip 27.0.0.1
```

config mobility secure-mode

To configure the secure mode for mobility messages between controllers, use the **config mobility secure-mode** command.

config mobility secure-mode {**enable** | **disable**}

Syntax Description

enable	Enables the mobility group message security.
disable	Disables mobility group message security.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the secure mode for mobility messages:

```
(Cisco Controller) >config mobility secure-mode enable
```

config mobility statistics reset

To reset the mobility statistics, use the **config mobility statistics reset** command.

config mobility statistics reset

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to reset the mobility group statistics:

```
(Cisco Controller) >config mobility statistics reset
```

config netuser add

To add a guest user on a WLAN or wired guest LAN to the local user database on the controller, use the **config netuser add** command.

config netuser add *username password* {**wlan** *wlan_id* | **guestlan** *guestlan_id*} **userType guest lifetime** *lifetime* **description** *description*

Syntax Description

username	Guest username. The username can be up to 50 alphanumeric characters.
password	User password. The password can be up to 24 alphanumeric characters.
wlan	Specifies the wireless LAN identifier to associate with or zero for any wireless LAN.
wlan_id	Wireless LAN identifier assigned to the user. A zero value associates the user with any wireless LAN.
guestlan	Specifies the guest LAN identifier to associate with or zero for any wireless LAN.
guestlan_id	Guest LAN ID.
userType	Specifies the user type.
guest	Specifies the guest for the guest user.
lifetime	Specifies the lifetime.
lifetime	Lifetime value (60 to 259200 or 0) in seconds for the guest user. **Note** A value of 0 indicates an unlimited lifetime.
description	Short description of user. The description can be up to 32 characters enclosed in double-quotes.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to add a permanent username Jane to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add jane able2 1 wlan_id 1 userType permanent
```

The following example shows how to add a guest username George to the wireless network for 1 hour:

```
(Cisco Controller) > config netuser add george able1 guestlan 1 3600
```

Related Commands

show netuser

config netuser delete

config netuser delete

To delete an existing user from the local network, use the **config netuser delete** command.

config netuser delete *username*

Syntax Description

username	Network username. The username can be up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Local network usernames must be unique because they are stored in the same database.

The following example shows how to delete an existing username named able1 from the network:

```
(Cisco Controller) > config netuser delete able1
Deleted user able1
```

Related Commands

show netuser

config netuser description

To add a description to an existing net user, use the **config netuser description** command.

config netuser description *username description*

Syntax Description

username	Network username. The username can contain up to 24 alphanumeric characters.
description	(Optional) User description. The description can be up to 32 alphanumeric characters enclosed in double quotes.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a user description “HQ1 Contact” to an existing network user named able 1:

```
(Cisco Controller) > config netuser description able1 “HQ1 Contact”
```

Related Commands

show netuser

config netuser guest-lan-id

To configure a wired guest LAN ID for a network user, use the **config netuser guest-lan-id** command.

config netuser guest-lan-id *username lan_id*

Syntax Description

username	Network username. The username can be 24 alphanumeric characters.
lan_id	Wired guest LAN identifier to associate with the user. A zero value associates the user with any wired LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a wired LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser guest- lan-id aire1 2
```

Related Commands

show netuser

show wlan summary

config netuser guest-role apply

To apply a quality of service (QoS) role to a guest user, use the **config netuser guest-role apply** command.

config netuser guest-role apply *username role_name*

Syntax Description

username	Name of the user.
role_name	QoS guest role name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you do not assign a QoS role to a guest user, the Role field in the User Details shows the role as default. The bandwidth contracts for this user are defined in the QoS profile for the WLAN.

If you want to unassign a QoS role from a guest user, use the **config netuser guest-role apply** *username* **default**. This user now uses the bandwidth contracts defined in the QoS profile for the WLAN.

The following example shows how to apply a QoS role to a guest user jsmith with the QoS guest role named Contractor:

```
(Cisco Controller) > config netuser guest-role apply jsmith Contractor
```

Related Commands

config netuser guest-role create

config netuser guest-role delete

config netuser guest-role create

To create a quality of service (QoS) role for a guest user, use the **config netuser guest-role create** command.

config netuser guest-role create *role_name*

Syntax Description

role name	QoS guest role name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To delete a QoS role, use the **config netuser guest-role delete** *role-name* .

The following example shows how to create a QoS role for the guest user named guestuser1:

```
(Cisco Controller) > config netuser guest-role create guestuser1
```

Related Commands

config netuser guest-role delete

config netuser guest-role delete

To delete a quality of service (QoS) role for a guest user, use the **config netuser guest-role delete** command.

config netuser guest-role delete *role_name*

Syntax Description

role name	Quality of service (QoS) guest role name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a quality of service (QoS) role for guestuser1:

```
(Cisco Controller) > config netuser guest-role delete guestuser1
```

Related Commands

config netuser guest-role create

config netuser guest-role qos data-rate average-data-rate

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-data-rate** command.

config netuser guest-role qos data-rate average-data-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average rate for the QoS guest named guestuser1:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-data-rate guestuser1
0
```

Related Commands

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

To configure the average data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate average-realtime-rate** command.

config netuser guest-role qos data-rate average-realtime-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Usage Guidelines

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure an average data rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate average-realtime-rate guestuser1
 0
```

Related Commands

config netuser guest-role

config netuser guest-role qos data-rate average-data-rate

config netuser guest-role qos data-rate burst-data-rate

To configure the peak data rate for TCP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-data-rate** command.

config netuser guest-role qos data-rate burst-data-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The burst data rate should be greater than or equal to the average data rate. Otherwise, the QoS policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure the peak data rate for the QoS guest named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-data-rate guestuser1 0
```

Related Commands

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

To configure the burst real-time data rate for UDP traffic on a per user basis, use the **config netuser guest-role qos data-rate burst-realtime-rate** command.

config netuser guest-role qos data-rate burst-realtime-rate *role_name rate*

Syntax Description

role_name	Quality of service (QoS) guest role name.
rate	Rate for TCP traffic on a per user basis.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The burst real-time rate should be greater than or equal to the average real-time rate. Otherwise, the quality of service (QoS) policy may block traffic to and from the wireless client.

For the *role_name* parameter in each of these commands, enter a name for the new QoS role. The name uniquely identifies the role of the QoS user (such as contractor, vendor, and so on.). For the *rate* parameter, you can enter a value between 0 and 60,000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS role.

The following example shows how to configure a burst real-time rate for the QoS guest user named guestuser1 with the rate for TCP traffic of 0 Kbps:

```
(Cisco Controller) > config netuser guest-role qos data-rate burst-realtime-rate guestuser1
 0
```

Related Commands

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

To configure the lifetime for a guest network user, use the **config netuser lifetime** command.

config netuser lifetime *username time*

Syntax Description

username	Network username. The username can be up to 50 alphanumeric characters.
time	Llifetime between 60 to 31536000 seconds or 0 for no limit.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure lifetime for a guest network user:

```
(Cisco Controller) > config netuser lifetime guestuser1 22450
```

Related Commands

show netuser

show wlan summary

config netuser maxUserLogin

To configure the maximum number of login sessions allowed for a network user, use the **config netuser maxUserLogin** command.

config netuser maxUserLogin *count*

Syntax Description

count	Maximum number of login sessions for a single user. The allowed values are from 0 (unlimited) to 8.

Command Default

By default, the maximum number of login sessions for a single user is 0 (unlimited).

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the maximum number of login sessions for a single user to 8:

```
(Cisco Controller) > config netuser maxUserLogin 8
```

Related Commands

show netuser

config netuser password

To change a local network user password, use the **config netuser password** command.

config netuser password *username password*

Syntax Description

username	Network username. The username can be up to 24 alphanumeric characters.
password	Network user password. The password can contain up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to change the network user password from aire1 to aire2:

```
(Cisco Controller) > config netuser password aire1 aire2
```

Related Commands

show netuser

config netuser wlan-id

To configure a wireless LAN ID for a network user, use the **config netuser wlan-id** command.

config netuser wlan-id *username wlan_id*

Syntax Description

username	Network username. The username can be 24 alphanumeric characters.
wlan_id	Wireless LAN identifier to associate with the user. A zero value associates the user with any wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to configure a wireless LAN ID 2 to associate with the user named aire1:

```
(Cisco Controller) > config netuser wlan-id aire1 2
```

Related Commands

show netuser

show wlan summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

The bridging shared secret is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

The following example shows how to configure the bridging shared secret string “shhh1”:

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

config network web-auth captive-bypass {**enable** | **disable**}

Syntax Description

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

show network summary

config network web-auth cmcc-support

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description

port	Port number. The valid range is from 0 to 65535.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands

show network summary

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {**enable** | **disable**}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb { **enable** | **disable** }

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.

Command Default

The default secure web (https) authentication for clients is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you configure the secure web (https) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the controller to implement the change.

The following example shows how to enable the secure web (https) authentication for clients:

```
(Cisco Controller) > config network web-auth secureweb enable
```

Related Commands

show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

config network webmode {**enable** | **disable**}

Syntax Description

enable	Enables the web interface.
disable	Disables the web interface.

Command Default

The default value for the web mode is **enable**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands

show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

Syntax Description

port	Configures additional ports for web authentication redirection.
port-number	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. **Note** Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

show run-config

config qos protocol-type

config network 802.3-bridging

To enable or disable 802.3 bridging on a controller, use the **config network 802.3-bridging** command.

config network 802.3-bridging {**enable** | **disable**}

Syntax Description

enable	Enables the 802.3 bridging.
disable	Disables the 802.3 bridging.

Command Default

By default, 802.3 bridging on the controller is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In controller software release 5.2, the software-based forwarding architecture for Cisco 2100 Series Controllers is being replaced with a new forwarding plane architecture. As a result, Cisco 2100 Series Controllers and the Cisco wireless LAN controller Network Module for Cisco Integrated Services Routers bridge 802.3 packets by default. Therefore, 802.3 bridging can now be disabled only on Cisco 4400 Series Controllers, the Cisco WiSM, and the Catalyst 3750G Wireless LAN Controller Switch.

To determine the status of 802.3 bridging, enter the **show netuser guest-roles** command.

The following example shows how to enable the 802.3 bridging:

```
(Cisco Controller) > config network 802.3-bridging enable
```

Related Commands

show netuser guest-roles

show network

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {**enable** | **disable**}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Command Default

Switch association is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an old bridge access point to associate with the switch:

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

config network ap-discovery nat-ip-only {**enable** | **disable**}

Syntax Description

enable	Enables use of NAT IP only in discovery response.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

The use of NAT IP only in discovery response is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

- If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.
- If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

  If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

  We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

The following example shows how to enable NAT IP in an AP discovery response:

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-easyadmin

To configure Cisco AP easyadmin feature, use the **config network ap-easyadmin** command.

config network ap-easyadmin {**enable** | **disable**}

Syntax Description

enable	Enables AP EasyAdmin.
disable	Disables AP EasyAdmin.

Command Default

The easyadmin is disabled by default.

Command History

Release	Modification
8.4	This command was introduced in this release

The following example shows how to enable the Cisco AP easyadmin:

```
(Cisco Controller) > config network ap-easyadmin enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco lightweight access point fallback.
disable	Disables the Cisco lightweight access point fallback.

Command Default

The Cisco lightweight access point fallback is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco lightweight access point fallback:

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {**enable** | **disable**}

Syntax Description

enable	Enables the lightweight access point priority reauthentication.
disable	Disables the lightweight access point priority reauthentication.

Command Default

The lightweight access point priority reauthentication is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {**enable** | **disable**}

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure AppleTalk bridging:

```
(Cisco Controller) > config network apple-talk enable
```

config network arptimeout

To set the Address Resolution Protocol (ARP) entry timeout value, use the **config network arptimeout** command.

config network arptimeout *seconds*

Syntax Description

seconds	Timeout in seconds. The minimum value is 10 seconds. The default value is 300 seconds.

Command Default

The default ARP entry timeout value is 300 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to set the ARP entry timeout value to 240 seconds:

```
(Cisco Controller) > config network arptimeout 240
```

Related Commands

show network summary

config assisted-roaming

To configure assisted roaming parameters on the controller, use the **config assisted-roaming** command.

config assisted-roaming {**denial-maximum** *count* | **floor-bias** *RSSI* | **prediction-minimum** *number_of_APs*}

Syntax Description

denial-maximum	Configures the maximum number of counts for association denial.
count	Maximum number of times that a client is denied for association when the association request that was sent to an access point does not match any access point on the prediction list. The range is from 1 to 10.
floor-bias	Configures the RSSI bias for access points on the same floor.
RSSI	RSSI bias for access points on the same floor. The range is from 5 to 25. Access points on the same floor have more preference.
prediction-minimum	Configures the minimum number of optimized access points for the assisted roaming feature.
number_of_APs	Minimum number of optimized access points for the assisted roaming feature. The range is from 1 to 6. If the number of access points in the prediction assigned to the client is smaller than this number, the assisted roaming feature does not work.

Command Default

The default RSSI bias for access points on the same floor is 15 dBm.

Usage Guidelines

802.11k allows a client to request a neighbor report that contains information about known neighbor access points, which can be used for a service set transition. The neighbor list reduces the need for active and passive scanning.

This example shows how to configure the minimum number of optimized access points for the assisted roaming feature:

```
(Cisco Controller) >config assisted-roaming prediction-minimum 4
```

config network allow-old-bridge-aps

To configure an old bridge access point's ability to associate with a switch, use the **config network allow-old-bridge-aps** command.

config network allow-old-bridge-aps {**enable** | **disable**}

Syntax Description

enable	Enables the switch association.
disable	Disables the switch association.

Command Default

Switch association is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an old bridge access point to associate with the switch:

```
(Cisco Controller) > config network allow-old-bridge-aps enable
```

config network ap-discovery

To enable or disable NAT IP in an AP discovery response, use the **config network ap-discovery** command.

config network ap-discovery nat-ip-only {**enable** | **disable**}

Syntax Description

enable	Enables use of NAT IP only in discovery response.
disable	Enables use of both NAT IP and non NAT IP in discovery response.

Command Default

The use of NAT IP only in discovery response is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

- If the **config interface nat-address management** command is set, this command controls which address(es) are sent in the CAPWAP discovery responses.
- If all APs are on the outside of the NAT gateway of the controller, enter the **config network ap-discovery nat-ip-only enable** command, and only the management NAT address is sent.
- If the controller has both APs on the outside and the inside of its NAT gateway, enter the **config network ap-discovery nat-ip-only disable** command, and both the management NAT address and the management inside address are sent. Ensure that you have entered the **config ap link-latency disable all** command to avoid stranding APs.
- If you disable **nat-ip-only**, the controller sends all active AP-Manager interfaces with their non-NAT IP in discovery response to APs.

  If you enable **nat-ip-only**, the controller sends all active AP-Manager interfaces with NAT IP if configured for the interface, else non-NAT IP.

  We recommend that you configure the interface as AP-Manager interface with NAT IP or non-NAT IP keeping these scenarios in mind because the AP chooses the least loaded AP-Manager interface received in the discovery response.

The following example shows how to enable NAT IP in an AP discovery response:

```
(Cisco Controller) > config network ap-discovery nat-ip-only enable
```

config network ap-fallback

To configure Cisco lightweight access point fallback, use the **config network ap-fallback** command.

config network ap-fallback {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco lightweight access point fallback.
disable	Disables the Cisco lightweight access point fallback.

Command Default

The Cisco lightweight access point fallback is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco lightweight access point fallback:

```
(Cisco Controller) > config network ap-fallback enable
```

config network ap-priority

To enable or disable the option to prioritize lightweight access points so that after a controller failure they reauthenticate by priority rather than on a first-come-until-full basis, use the **config network ap-priority** command.

config network ap-priority {**enable** | **disable**}

Syntax Description

enable	Enables the lightweight access point priority reauthentication.
disable	Disables the lightweight access point priority reauthentication.

Command Default

The lightweight access point priority reauthentication is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the lightweight access point priority reauthorization:

```
(Cisco Controller) > config network ap-priority enable
```

config network apple-talk

To configure AppleTalk bridging, use the **config network apple-talk** command.

config network apple-talk {**enable** | **disable**}

Syntax Description

enable	Enables the AppleTalk bridging.
disable	Disables the AppleTalk bridging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure AppleTalk bridging:

```
(Cisco Controller) > config network apple-talk enable
```

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

The bridging shared secret is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

The following example shows how to configure the bridging shared secret string “shhh1”:

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network bridging-shared-secret

To configure the bridging shared secret, use the **config network bridging-shared-secret** command.

config network bridging-shared-secret *shared_secret*

Syntax Description

shared_secret	Bridging shared secret string. The string can contain up to 10 bytes.

Command Default

The bridging shared secret is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command creates a secret that encrypts backhaul user data for the mesh access points that connect to the switch.

The zero-touch configuration must be enabled for this command to work.

The following example shows how to configure the bridging shared secret string “shhh1”:

```
(Cisco Controller) > config network bridging-shared-secret shhh1
```

Related Commands

show network summary

config network broadcast

To enable or disable broadcast packet forwarding, use the **config network broadcast** command.

config network broadcast {**enable** | **disable**}

Syntax Description

enable	Enables the broadcast packet forwarding.
disable	Disables the broadcast packet forwarding.

Command Default

The broadcast packet forwarding is disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command allows you to enable or disable broadcasting. You must enable multicast mode before enabling broadcast forwarding. Use the **config network multicast mode command** to configure multicast mode on the controller.

Note The default multicast mode is unicast in case of all controllers except for Cisco 2106 Controllers. The broadcast packets and multicast packets can be independently controlled. If multicast is off and broadcast is on, broadcast packets still reach the access points, based on the configured multicast mode.

The following example shows how to enable broadcast packet forwarding:

```
(Cisco Controller) > config network broadcast enable
```

Related Commands

show network summary

config network multicast global

config network multicast mode

config network fast-ssid-change

To enable or disable fast Service Set Identifier (SSID) changing for mobile stations, use the **config network fast-ssid-change** command.

config network fast-ssid-change {**enable** | **disable**}

Syntax Description

enable	Enables the fast SSID changing for mobile stations
disable	Disables the fast SSID changing for mobile stations.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable the Fast SSID Change feature, the controller allows clients to move between SSIDs. When the client sends a new association for a different SSID, the client entry in the controller connection table is cleared before the client is added to the new SSID.

When you disable the FastSSID Change feature, the controller enforces a delay before clients are allowed to move to a new SSID.

The following example shows how to enable the fast SSID changing for mobile stations:

```
(Cisco Controller) > config network fast-ssid-change enable
```

Related Commands

show network summary

config network ip-mac-binding

To validate the source IP address and MAC address binding within client packets, use the **config network ip-mac-binding** command.

config network ip-network-binding {**enable** | **disable**}

Syntax Description

enable	Enables the validation of the source IP address to MAC address binding in clients packets.
disable	Disables the validation of the source IP address to MAC address binding in clients packets.

Command Default

The validation of the source IP address to MAC address binding in clients packets is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In controller software release 5.2, the controller enforces strict IP address-to-MAC address binding in client packets. The controller checks the IP address and MAC address in a packet, compares them to the addresses that are registered with the controller, and forwards the packet only if they both match. In previous releases, the controller checks only the MAC address of the client and ignores the IP address.

Note You might want to disable this binding check if you have a routed network behind a workgroup bridge (WGB).

The following example shows how to validate the source IP and MAC address within client packets:

```
(Cisco Controller) > config network ip-mac-binding enable
```

config network link local bridging

To configure bridging of link local traffic at the local site, use the **config network link-local-bridging** command.

config network link-local-bridging {**enable** | **disable**}

Syntax Description

enable	Enables bridging of link local traffic at the local site
disable	Disables bridging of link local traffic at the local site

Command Default

Disabled

Command History

Release	Modification
8.0	This command was introduced

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default primary, use the **config network master-base** command.

config network master-base {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the primary Cisco wireless LAN controller is normally not used in a deployed network, the primary Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

The following example shows how to enable the Cisco wireless LAN controller as a default primary:

```
(Cisco Controller) > config network master-base enable
```

config network mgmt-via-wireless

To enable Cisco wireless LAN controller management from an associated wireless client, use the **config network mgmt-via-wireless** command.

config network mgmt-via-wireless {**enable** | **disable**}

Syntax Description

enable	Enables the switch management from a wireless interface.
disable	Disables the switch management from a wireless interface.

Command Default

The switch management from a wireless interface is disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This feature allows wireless clients to manage only the Cisco wireless LAN controller associated with the client and the associated Cisco lightweight access point. That is, clients cannot manage another Cisco wireless LAN controller with which they are not associated.

This example shows how to configure switch management from a wireless interface:

```
(Cisco Controller) > config network mgmt-via-wireless enable
```

Related Commands

show network summary

config network multicast global

To enable or disable multicasting on the controller, use the **config network multicast global** command.

config network multicast global {**enable** | **disable**}

Syntax Description

enable	Enables the multicast global support.
disable	Disables the multicast global support.

Command Default

Multicasting on the controller is disabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The **config network broadcast** {**enable** | **disable**} command allows you to enable or disable broadcasting without enabling or disabling multicasting as well. This command uses the multicast mode configured on the controller (by using the **config network multicast mode command)** to operate.

The following example shows how to enable the global multicast support:

```
(Cisco Controller) > config network multicast global enable
```

Related Commands

show network summary

config network broadcast

config network multicast mode

config network multicast igmp query interval

To configure the IGMP query interval, use the **config network multicast igmp query interval** command.

config network multicast igmp query interval *value*

Syntax Description

value	Frequency at which controller sends IGMP query messages. The range is from 15 to 2400 seconds.

Command Default

The default IGMP query interval is 20 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To configure IGMP query interval, ensure that you do the following:

- Enable the global multicast by entering the **config network multicast global enable** command.
- Enable IGMP snooping by entering the **config network multicast igmp snooping enable** command.

The following example shows how to configure the IGMP query interval at 20 seconds:

```
(Cisco Controller) > config network multicast igmp query interval 20
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp timeout

config network multicast igmp snooping

To enable or disable IGMP snooping, use the **config network multicast igmp snooping** command.

config network multicast igmp snooping {**enable** | **disable**}

Syntax Description

enable	Enables IGMP snooping.
disable	Disables IGMP snooping.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable internet IGMP snooping settings:

```
(Cisco Controller) > config network multicast igmp snooping enable
```

Related Commands

config network multicast global

config network multicast igmp query interval

config network multicast igmp timeout

config network multicast igmp timeout

To set the IGMP timeout value, use the **config network multicast igmp timeout** command.

config network multicast igmp timeout *value*

Syntax Description

value	Timeout range from 30 to 7200 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can enter a timeout value between 30 and 7200 seconds. The controller sends three queries in one timeout value at an interval of timeout/3 to see if any clients exist for a particular multicast group. If the controller does not receive a response through an IGMP report from the client, the controller times out the client entry from the MGID table. When no clients are left for a particular multicast group, the controller waits for the IGMP timeout value to expire and then deletes the MGID entry from the controller. The controller always generates a general IGMP query (to destination address 224.0.0.1) and sends it on all WLANs with an MGID value of 1.

The following example shows how to configure the timeout value 50 for IGMP network settings:

```
(Cisco Controller) > config network multicast igmp timeout 50
```

Related Commands

config network multicast global

config network igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

To configure the Layer 2 multicast on an interface or all interfaces, use the **config network multicast l2mcast** command.

config network multicast l2mcast {**enable** | **disable** {**all** | *interface-name*}

Syntax Description

enable	Enables Layer 2 multicast.
disable	Disables Layer 2 multicast.
all	Applies to all interfaces.
interface-name	Interface name for which the Layer 2 multicast is to enabled or disabled.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable Layer 2 multicast for all interfaces:

```
(Cisco Controller) > config network multicast l2mcast enable all
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast mld

config network multicast mld

To configure the Multicast Listener Discovery (MLD) parameters, use the **config network multicast mld** command.

config network multicast mld {**query interval** *interval-value* | **snooping** {**enable** | **disable**} | **timeout** *timeout-value*}

Syntax Description

query interval	Configures query interval to send MLD query mess
interval-value	Query interval in seconds. The range is from 15 to
snooping	Configures MLD snooping.
enable	Enables MLD snooping.
disable	Disables MLD snooping.
timeout	Configures MLD timeout.
timeout-value	Timeout value in seconds. The range is from 30 secon

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set a query interval of 20 seconds for MLD query messages:

```
(Cisco Controller) > config network multicast mld query interval 20
```

Related Commands

config network multicast global

config network multicast igmp snooping

config network multicast igmp query interval

config network multicast l2mcast

config network multicast mode multicast

To configure the controller to use the multicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode multicast** command.

config network multicast mode multicast

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the multicast mode to send a single copy of data to multiple receivers:

```
(Cisco Controller) > config network multicast mode multicast
```

Related Commands

config network multicast global

config network broadcast

config network multicast mode unicast

config network multicast mode unicast

To configure the controller to use the unicast method to send broadcast or multicast packets to an access point, use the **config network multicast mode unicast** command.

config network multicast mode unicast

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the controller to use the unicast mode:

```
(Cisco Controller) > config network multicast mode unicast
```

Related Commands

config network multicast global

config network broadcast

config network multicast mode multicast

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

Syntax Description

enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.

Command Default

The Ethernet port 3 Cisco 600 Series OEAP is reset.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network oeap-600 local-network** command.

config network oeap-600 local-network {**enable** | **disable**}

Syntax Description

enable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.
disable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default

Access to the local network for the Cisco 600 Series OEAPs is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {**enable** | **disable**}

Syntax Description

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Command Default

The OTAP provisioning is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the OTAP provisioning:

```
(Cisco Controller) >config network otap-mode disable
```

config network profiling

To profile http port for a specific port, use the **config network profiling http-port** command.

config network profiling http-port *port number*

Syntax Description

port number	Interface port number. Default value is 80.

Command History

Release	Modification
8.2	This command was introduced

The following example shows how to configure the http port in a network:

```
(Cisco Controller) > config network profiling http-port 80
```

config network rf-network-name

To set the RF-Network name, use the **config network rf-network-name** command.

config network rf-network-name *name*

Syntax Description

name	RF-Network name. The name can contain up to 19 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the RF-network name to travelers:

```
(Cisco Controller) > config network rf-network-name travelers
```

Related Commands

show network summary

config network secureweb

To change the state of the secure web (https is http and SSL) interface for management users, use the **config network secureweb** command.

config network secureweb {**enable** | **disable**}

Syntax Description

enable	Enables the secure web interface for management users.
disable	Disables the secure web interface for management users.

Command Default

The secure web interface for management users is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command allows management users to access the controller GUI using an http://ip-address. Web mode is not a secure connection.

The following example shows how to enable the secure web interface settings for management users:

```
(Cisco Controller) > config network secureweb enable
You must reboot for the change to take effect.
```

Related Commands

config network secureweb cipher-option

show network summary

config network secureweb cipher-option

To enable or disable secure web mode with increased security, or to enable or disable Secure Sockets Layer (SSL v2) for web administration and web authentication, use the **config network secureweb cipher-option** command.

config network secureweb cipher-option {**high** | **sslv2** | **rc4-preference**} {**enable** | **disable**}

Syntax Description

high	Configures whether or not 128-bit ciphers are required for web administration and web authentication.
sslv2	Configures SSLv2 for both web administration and web authentication.
rc4-preference	Configures preference for RC4-SHA (Rivest Cipher 4-Secure Hash Algorithm) cipher suites (over CBC cipher suites) for web authentication and web administration.
enable	Enables the secure web interface.
disable	Disables the secure web interface.

Command Default

The default is **disable** for secure web mode with increased security and **enable** for SSL v2.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Note The **config network secureweb cipher-option** command allows users to access the controller GUI using an http://ip-address but only from browsers that support 128-bit (or larger) ciphers.

When cipher-option sslv2 is disabled, users cannot connect using a browser configured with SSLv2 only. They must use a browser that is configured to use a more secure protocol such as SSLv3 or later.

In RC4-SHA based cipher suites, RC4 is used for encryption and SHA is used for message authentication.

The following example shows how to enable secure web mode with increased security:

```
(Cisco Controller) > config network secureweb cipher-option
```

The following example shows how to disable SSL v2:

```
(Cisco Controller) > config network secureweb cipher-option sslv2 disable
```

Related Commands

config network secureweb

show network summary

config network ssh

To allow or disallow new Secure Shell (SSH) sessions, use the **config network ssh** command.

config network ssh {**enable** | **disable**}

Syntax Description

enable	Allows the new SSH sessions.
disable	Disallows the new SSH sessions.

Command Default

The default value for the new SSH session is **disable**.

The following example shows how to enable the new SSH session:

```
(Cisco Controller) > config network ssh enable
```

Related Commands

show network summary

config network telnet

To allow or disallow new Telnet sessions, use the **config network telnet** command.

config network telnet {**enable** | **disable**}

Syntax Description

enable	Allows new Telnet sessions.
disable	Disallows new Telnet sessions.

Command Default

By default, the new Telnet session is disallowed and the value is **disable**.

Usage Guidelines

Telnet is not supported on Cisco Aironet 1830 and 1850 Series Access Points.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the new Telnet sessions:

```
(Cisco Controller) > config network telnet enable
```

Related Commands

config ap telnet

show network summary

config network usertimeout

To change the timeout for idle client sessions, use the **config network usertimeout** command.

config network usertimeout *seconds*

Syntax Description

seconds	Timeout duration in seconds. The minimum value is 90 seconds. The default value is 300 seconds.

Command Default

The default timeout value for idle client session is 300 seconds.

Usage Guidelines

Use this command to set the idle client session duration on the Cisco wireless LAN controller. The minimum duration is 90 seconds.

The following example shows how to configure the idle session timeout to 1200 seconds:

```
(Cisco Controller) > config network usertimeout 1200
```

Related Commands

show network summary

config network web-auth captive-bypass

To configure the controller to support bypass of captive portals at the network level, use the **config network web-auth captive-bypass** command.

config network web-auth captive-bypass {**enable** | **disable**}

Syntax Description

enable	Allows the controller to support bypass of captive portals.
disable	Disallows the controller to support bypass of captive portals.

Command Default

None

The following example shows how to configure the controller to support bypass of captive portals:

```
(Cisco Controller) > config network web-auth captive-bypass enable
```

Related Commands

show network summary

config network web-auth cmcc-support

config network web-auth cmcc-support

To configure eWalk on the controller, use the **config network web-auth cmcc-support** command.

config network web-auth cmcc-support {**enable** | **disable**}

Syntax Description

enable	Enables eWalk on the controller.
disable	Disables eWalk on the controller.

Command Default

None

The following example shows how to enable eWalk on the controller:

```
(Cisco Controller) > config network web-auth cmcc-support enable
```

Related Commands

show network summary

config network web-auth captive-bypass

config network web-auth port

To configure an additional port to be redirected for web authentication at the network level, use the **config network web-auth port** command.

config network web-auth port *port*

Syntax Description

port	Port number. The valid range is from 0 to 65535.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an additional port number 1200 to be redirected for web authentication:

```
(Cisco Controller) > config network web-auth port 1200
```

Related Commands

show network summary

config network web-auth proxy-redirect

To configure proxy redirect support for web authentication clients, use the **config network web-auth proxy-redirect** command.

config network web-auth proxy-redirect {**enable** | **disable**}

Syntax Description

enable	Allows proxy redirect support for web authentication clients.
disable	Disallows proxy redirect support for web authentication clients.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

config network web-auth secureweb

To configure the secure web (https) authentication for clients, use the **config network web-auth secureweb** command.

config network web-auth secureweb { **enable** | **disable** }

Syntax Description

enable	Allows secure web (https) authentication for clients.
disable	Disallows secure web (https) authentication for clients. Enables http web authentication for clients.

Command Default

The default secure web (https) authentication for clients is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you configure the secure web (https) authentication for clients using the **config network web-auth secureweb disable** command, then you must reboot the controller to implement the change.

The following example shows how to enable the secure web (https) authentication for clients:

```
(Cisco Controller) > config network web-auth secureweb enable
```

Related Commands

show network summary

config network web-auth https-redirect

To configure https redirect support for web authentication clients, use the **config network web-auth https-redirect** command.

config network web-auth https-redirect {**enable** | **disable**}

Syntax Description

enable	Enables the secure redirection(https) for web-authentication clients.
disable	Disables the secure redirection(https) for web-authentication clients.

Command Default

This command is by default disabled.

Command History

Release	Modification
8.0	This command was introduced in Release 8.0

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth https-redirect enable
```

Related Commands

show network summary

config network webmode

To enable or disable the web mode, use the **config network webmode** command.

config network webmode {**enable** | **disable**}

Syntax Description

enable	Enables the web interface.
disable	Disables the web interface.

Command Default

The default value for the web mode is **enable**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the web interface mode:

```
(Cisco Controller) > config network webmode disable
```

Related Commands

show network summary

config network web-auth

To configure the network-level web authentication options, use the **config network web-auth** command.

config network web-auth {**port** *port-number*} | {**proxy-redirect** {**enable** | **disable**}}

Syntax Description

port	Configures additional ports for web authentication redirection.
port-number	Port number (between 0 and 65535).
proxy-redirect	Configures proxy redirect support for web authentication clients.
enable	Enables proxy redirect support for web authentication clients. **Note** Web-auth proxy redirection will be enabled for ports 80, 8080, and 3128, along with user defined port 345.
disable	Disables proxy redirect support for web authentication clients.

Command Default

The default network-level web authentication value is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must reset the system for the configuration to take effect.

The following example shows how to enable proxy redirect support for web authentication clients:

```
(Cisco Controller) > config network web-auth proxy-redirect enable
```

Related Commands

show network summary

show run-config

config qos protocol-type

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {**enable** | **disable**}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Command Default

The bridge access point ZeroConfig support is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the bridge access point ZeroConfig support:

```
(Cisco Controller) >config network zero-config enable
```

config network master-base

To enable or disable the Cisco wireless LAN controller as an access point default primary, use the **config network master-base** command.

config network master-base {**enable** | **disable**}

Syntax Description

enable	Enables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.
disable	Disables the Cisco wireless LAN controller acting as a Cisco lightweight access point default primary.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This setting is only used upon network installation and should be disabled after the initial network configuration. Because the primary Cisco wireless LAN controller is normally not used in a deployed network, the primary Cisco wireless LAN controller setting can be saved from 6.0.199.0 or later releases.

The following example shows how to enable the Cisco wireless LAN controller as a default primary:

```
(Cisco Controller) > config network master-base enable
```

config network oeap-600 dual-rlan-ports

To configure the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4, use the **config network oeap-600 dual-rlan-ports** command.

config network oeap-600 dual-rlan-ports {**enable** | **disable**}

Syntax Description

enable	Enables Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port in addition to port 4.
disable	Resets the Ethernet port 3 Cisco OfficeExtend 600 Series access points to function as a local LAN port.

Command Default

The Ethernet port 3 Cisco 600 Series OEAP is reset.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Ethernet port 3 of Cisco OfficeExtend 600 Series access points to operate as a remote LAN port:

```
(Cisco Controller) > config network oeap-600 dual-rlan-ports enable
```

config network oeap-600 local-network

To configure access to the local network for the Cisco 600 Series OfficeExtend access points, use the **config network oeap-600 local-network** command.

config network oeap-600 local-network {**enable** | **disable**}

Syntax Description

enable	Enables access to the local network for the Cisco 600 Series OfficeExtend access points.
disable	Disables access to the local network for the Cisco 600 Series OfficeExtend access points.

Command Default

Access to the local network for the Cisco 600 Series OEAPs is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable access to the local network for the Cisco 600 Series OfficeExtend access points:

```
(Cisco Controller) > config network oeap-600 local-network enable
```

config network otap-mode

To enable or disable over-the-air provisioning (OTAP) of Cisco lightweight access points, use the **config network otap-mode** command.

config network otap-mode {**enable** | **disable**}

Syntax Description

enable	Enables the OTAP provisioning.
disable	Disables the OTAP provisioning.

Command Default

The OTAP provisioning is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the OTAP provisioning:

```
(Cisco Controller) >config network otap-mode disable
```

config network zero-config

To configure bridge access point ZeroConfig support, use the **config network zero-config** command.

config network zero-config {**enable** | **disable**}

Syntax Description

enable	Enables the bridge access point ZeroConfig support.
disable	Disables the bridge access point ZeroConfig support.

Command Default

The bridge access point ZeroConfig support is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the bridge access point ZeroConfig support:

```
(Cisco Controller) >config network zero-config enable
```

config nmsp notify-interval measurement

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **config nmsp notify-interval measurement** command.

config nmsp notify-interval measurement {**client** | **rfid** | **rogue**} *interval*

Syntax Description

client	Modifies the interval for clients.
rfid	Modifies the interval for active radio frequency identification (RFID) tags.
rogue	Modifies the interval for rogue access points and rogue clients.
interval	Time interval. The range is from 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The TCP port (16113) that the controller and location appliance communicate over must be open (not blocked) on any firewall that exists between the controller and the location appliance for NMSP to function.

The following example shows how to modify the NMSP notification interval for the active RFID tags to 25 seconds:

```
(Cisco Controller) > config nmsp notify-interval measurement rfid 25
```

Related Commands

clear locp statistics

clear nmsp statistics

show nmsp notify-interval summary

show nmsp statistics

show nmsp status

config opendns

To enable or disable open Domain Name System (DNS) on the controller, use the **config opendns**command.

config opendns { **enable** | **disable** }

Syntax Description

enable	Enables the opendns global configuration.
disable	Disables the opendns global configuration.

Command Default

Open DNS is not configured.

Command Modes

Controller Config >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable open DNS on the controller:

```
(Cisco Controller) > config opendns enable
```

config opendns api-token

To enable or disable OpenDNS API token help for registering on the controller, use the **config opendns api-token** command.

config opendns api-token *api-token*

Syntax Description

api-token	API token for the OpenDNS.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable API token help for registering OpenDNS on the controller:

```
(Cisco Controller) > config opendns api-token 12
```

config opendns forced

To enable or disable OpenDNS on the controller, use the **config opendns forced** command.

config opendns forced {**enable** | **disable**}

Syntax Description

enable	Enables the OpenDNS global configuration.
disable	Disables the OpenDNS global configuration.

Command Default

OpenDNS is not configured.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to enable OpenDNS on the controller:

```
(Cisco Controller) > config opendns forced enable
```

config opendns profile

To configure a profile for the OpenDNS, which can be applied to a user group, or wireless LAN (WLAN), or site, use the **config opendns profile** command.

config opendns profile { **create** | **delete** | **refresh** } *profile-name*

Syntax Description

create	Creates an OpenDNS identity name.
delete	Removes an OpenDNS identity name.
refresh	Refreshes OpenDNS identity by retriggering the registration, irrespective of current state.
profile-name	OpenDNS identity name.

Command Default

OpenDNS profile is not created.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure a profile for OpenDNS, which can be applied to a user group:

```
(Cisco Controller) > config opendns profile create usergroup1
```

config pmipv6 domain

To configure PMIPv6 and to enable Mobile Access Gateway (MAG) functionality on controller, use the **config pmipv6 domain** command.

config pmipv6 domain *domain_name*

Syntax Description

domain_name	Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a domain name for a PMIPv6 WLAN:

```
(Cisco Controller) >config pmipv6 domain floor1
```

config pmipv6 add profile

To create a Proxy Mobility IPv6 (PMIPv6) profile for the WLAN, use the **config pmipv6 add profile** command. You can configure PMIPv6 profiles based on a realm or a service set identifier (SSID).

config pmipv6 add profile *profile_name* **nai** {*user@realm* | *@realm* | *****} **lma** *lma_name* **apn** *apn_name*

Syntax Description

profile_name	Name of the profile. The profile name is case sensitive and can be up to 127 alphanumeric characters.
nai	Specifies the Network Access Identifier of the client.
user@realm	Network Access Identifier of the client in the format *user*@realm. The NAI name is case sensitive and can be up to 127 alphanumeric characters.
@realm	Network Access Identifier of the client in the format @realm.
*****	All Network Access Identifiers. You can have profiles based on an SSID for all users.
lma	Specifies the Local Mobility Anchor (LMA).
lma_name	Name of LMA. The LMA name is case sensitive and can be up to 127 alphanumeric characters.
apn	Specifies the access point.
ap_name	Name of the access point. The access point name is case sensitive and can be up to 127 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command is a prerequisite for using PMIPv6 configuration commands if the controller uses open authentication.

The following example shows how to create a PMIPv6 profile:

```
(Cisco Controller) >config pmipv6 add profile profile1 nai @vodfone.com lma vodfonelma apn
 vodafoneapn
```

config pmipv6 delete

To delete a Proxy Mobility IPv6 (PMIPv6) profile, domain, or Local Mobility Anchor (LMA), use the **config pmipv6 delete** command.

config pmipv6 delete {**profile** *profile_name* **nai** { *nai_id* | **all** } | **domain** *domain_name* | **lma** *lma_name*}

Syntax Description

profile	Specifies the PMIPv6 profile.
profile_name	Name of the PMIPv6 profile. The profile name is case sensitive and can be up to 127 alphanumeric characters.
nai	Specifies the Network Access Identifier (NAI) of a mobile client.
nai_id	Network Access Identifier of a mobile client. The NAI is case sensitive and can be up to 127 alphanumeric characters.
all	Specifies all NAIs. When you delete all NAIs, the profile is deleted.
domain	Specifies the PMIPv6 domain.
domain_name	Name of the PMIPv6 domain. The domain name is case sensitive and can be up to 127 alphanumeric characters.
lma	Specifies the LMA.
lma_name	Name of the LMA. The LMA name is case sensitive and can be up to 127 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a domain:

```
(Cisco Controller) >config pmipv6 delete lab1
```

config pmipv6 mag apn

To configure an Access Point Name (APN) for a mobile access gateway (MAG), use the **config pmipv6 mag apn** command.

config pmipv6 mag apn *apn-name*

Syntax Description

apn-name	Access point name for the MAG.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

By default, the MAG role is WLAN. However, for the lightweight access points, MAG role should be configured as 3GPP. If the MAG role is 3GPP, it is mandatory to specify an APN for the MAG.

To delete an APN for a MAG, use the **config pmipv6 delete mag apn** *apn-name* command.

The following example shows how to add an APN for a MAG:

```
(Cisco Controller) >config pmipv6 mag apn myCiscoAP
```

config pmipv6 mag binding init-retx-time

To configure the initial timeout between the proxy binding updates (PBUs) when the Mobile Access Gateway (MAG) does not receive the proxy binding acknowledgements (PBAs), use the **config pmipv6 mag binding init-retx-time** command.

config pmipv6 mag binding init-retx-time *units*

Syntax Description

units	Initial timeout between the PBUs when the MAG does not receive the PBAs. The range is from 100 to 65535 seconds.

Command Default

The default initial timeout is 1000 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the initial timeout between the PBUs when the MAG does not receive the PBAs:

```
(Cisco Controller) >config pmipv6 mag binding init-retx-time 500
```

config pmipv6 mag binding lifetime

To configure the lifetime of the binding entries in the Mobile Access Gateway (MAG), use the **config pmipv6 mag binding lifetime** command.

config pmipv6 mag binding lifetime *units*

Syntax Description

units	Lifetime of the binding entries in the MAG. The binding lifetime must be a multiple of 4 seconds. The range is from 10 to 65535 seconds.

Command Default

The default lifetime of the binding entries is 65535 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must configure a Proxy Mobility IPv6 (PMIPv6) domain before you configure the lifetime of the binding entries in the controller.

The following example shows how to configure the lifetime of the binding entries in the controller:

```
(Cisco Controller) >config pmipv6 mag binding lifetime 5000
```

config pmipv6 mag binding max-retx-time

To configure the maximum timeout between the proxy binding updates (PBUs) when the Mobility Access Gateway (MAG) does not receive the proxy binding acknowledgments (PBAs), use the **config pmipv6 mag binding max-retx-time** command.

config pmipv6 mag binding max-retx-time *units*

Syntax Description

units	Maximum timeout between the PBUs when the MAG does not receive the PBAs. The range is from 100 to 65535 seconds.

Command Default

The default maximum timeout is 32000 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the maximum timeout between the PBUs when the MAG does not receive the PBAs:

```
(Cisco Controller) >config pmipv6 mag binding max-retx-time 50
```

config pmipv6 mag binding maximum

To configure the maximum number of binding entries in the Mobile Access Gateway (MAG), use the **config pmipv6 mag binding maximum** command.

config pmipv6 mag binding maximum *units*

Syntax Description

units	Maximum number of binding entries in the MAG. This number indicates the maximum number of users connected to the MAG. The range is from 0 to 40000.

Command Default

The default maximum number of binding entries in the MAG is 10000.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must configure a Proxy Mobility IPv6 (PMIPv6) domain before you configure the maximum number of binding entries in the MAG.

The following example shows how to configure the maximum number of binding entries in the MAG:

```
(Cisco Controller) >config pmipv6 mag binding maximum 20000
```

config pmipv6 mag binding refresh-time

To configure the refresh time of the binding entries in the MAG, use the **config pmipv6 mag binding refresh-time** command.

config pmipv6 mag binding refresh-time *units*

Syntax Description

units	Refresh time of the binding entries in the MAG. The binding refresh time must be a multiple of 4. The range is from 4 to 65535 seconds.

Command Default

The default refresh time of the binding entries in the MAG is 300 seconds.

Usage Guidelines

You must configure a PMIPv6 domain before you configure the refresh time of the binding entries in the MAG.

The following example shows how to configure the refresh time of the binding entries in the MAG:

```
(Cisco Controller) >config pmipv6 mag binding refresh-time 500
```

config pmipv6 mag bri delay

To configure the maximum or minimum amount of time that the MAG waits before retransmitting a Binding Revocation Indication (BRI) message, use the **config pmipv6 mag bri delay** command.

config pmipv6 mag bri delay {**min** | **max**} *time*

Syntax Description

min	Specifies the minimum amount of time that the MAG waits before retransmitting a BRI message.
max	Specifies the maximum amount of time that the MAG waits before retransmitting a BRI message.
time	Maximum or minimum amount of time that the controller waits before retransmitting a BRI message. The range is from 500 to 65535 milliseconds.

Command Default

The default value of the maximum amount of time that the MAG waits before retransmitting a BRI message is 2 seconds.

The default value of the minimum amount of time that the MAG waits before retransmitting a BRI message is 1 second.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the minimum amount of time that the MAG waits before retransmitting a BRI message:

```
(Cisco Controller) >config pmipv6 mag bri delay min 500
```

config pmipv6 mag bri retries

To configure the maximum number of times that the MAG retransmits the Binding Revocation Indication (BRI) message before receiving the Binding Revocation Acknowledgment (BRA) message, use the **config pmipv6 mag bri retries** command.

config pmipv6 mag bri retries *retries*

Syntax Description

retries	Maximum number of times that the MAG retransmits the BRI message before receiving the BRA message. The range is from 1 to 10 retries.

Command Default

The default is 1 retry.

The following example shows how to configure the maximum number of times that the MAG retries:

```
(Cisco Controller) >config pmipv6 mag bri retries 5
```

config pmipv6 mag lma

To configure a local mobility anchor (LMA) with the mobile access gateway (MAG), use the **config pmipv6 mag lma** command.

config pmipv6 mag lma *lma_name* **ipv4-address** *address*

Syntax Description

lma_name	Name of the LMA. The LMA name can be a NAI or a string that uniquely identifies the LMA.
ipv4-address	Specifies the IP address of the LMA.
address	IP address of the LMA.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command is a prerequisite to configure PMIPv6 parameters on the MAG.

The following example shows how to configure an LMA with the MAG:

```
(Cisco Controller) >config pmipv6 mag lma vodafonelma ipv4-address 209.165.200.254
```

config pmipv6 mag replay-protection

To configure the maximum amount of time difference between the timestamp in the received proxy binding acknowledgment (PBA) and the current time of the day for replay protection, use the **config pmipv6 mag replay-protection** command.

config pmipv6 mag replay-protection { **timestamp window** *time* | **sequence-no** *sequence* | **mobile-node-timestamp** *mobile_node_timestamp* }

Syntax Description

timestamp	Specifies the time stamp of the PBA message.
window	Specifies the maximum time difference between the time stamp in the received PBA message and the current time of day.
time	Maximum time difference between the time stamp in the received PBA message and the current time of day. The range is from 1 to 300 milliseconds.
sequence-no	(Optional) Specifies the sequence number in a Proxy Binding Update message.
sequence	(Optional) Sequence number in the Proxy Binding Update message.
mobile_node_timestamp	(Optional) Specifies the time stamp of the mobile node.
mobile_node_timestamp	(Optional) Time stamp of the mobile node.

Command Default

The default maximum time difference is 300 milliseconds.

Usage Guidelines

Only the timestamp option is supported.

The following example shows how to configure the maximum amount of time difference in milliseconds between the time stamp in the received PBA message and the current time of day:

```
(Cisco Controller) >config pmipv6 mag replay-protection timestamp window 200
```

config port power

To enable or disable Power over Ethernet (PoE) for a specific controller port or for all ports, use the **config port power** command.

config port power {**all** | *port*} {**enable** | **disable**}

Syntax Description

all	Configures all ports.
port	Port number.
enable	Enables the specified ports.
disable	Disables the specified ports.

Command Default

Enabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable PoE on all ports:

```
(Cisco Controller) > config port power all enable
```

The following example shows how to disable PoE on port 8:

```
(Cisco Controller) > config port power 8 disable
```

config policy action opendns-profile-name

To configure an OpenDNS action to a policy, use the **config policy action opendns-profile-name** command.

config policy *policy-name* **action opendns-profile-name** {**enable** | **disable**}

Syntax Description

policy-name	Policy name, for example, iPad, iPhone, smartphone.
enable	Enables the action.
disable	Disables the action.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure an OpenDNS action to a policy:

```
(Cisco Controller) > config policy ipad action opendns-profile-name enable
```

config paging

To enable or disable scrolling of the page, use the **config paging** command.

config paging {**enable** | **disable**}

Syntax Description

enable	Enables the scrolling of the page.
disable	Disables the scrolling of the page.

Command Default

By default, scrolling of the page is enabled.

Usage Guidelines

Commands that produce a huge number of lines of output with the scrolling of the page disabled might result in the termination of SSH/Telnet connection or user session on the console.

The following example shows how to enable scrolling of the page:

```
(Cisco Controller) > config paging enable
```

Related Commands

show run-config

config passwd-cleartext

To enable or disable temporary display of passwords in plain text, use the **config passwd-cleartext** command.

config passwd-cleartext {**enable** | **disable**}

Syntax Description

enable	Enables the display of passwords in plain text.
disable	Disables the display of passwords in plain text.

Command Default

By default, temporary display of passwords in plain text is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be enabled if you want to see user-assigned passwords displayed in clear text when using the **show run-config** command.

To execute this command, you must enter an admin password. This command is valid only for this particular session. It is not saved following a reboot.

The following example shows how to enable display of passwords in plain text:

```
(Cisco Controller) > config passwd-cleartext enable
The way you see your passwds will be changed
You are being warned.
Enter admin password:
```

Related Commands

show run-config

config policy

To configure a native profiling policy on the controller, use the **config policy** command.

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** | **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**}}

Syntax Description

policy_name	Name of a profiling policy.
action	Configures an action for the policy.
acl	Configures an ACL for the policy
enable	Enables an action for the policy.
disable	Disables an action for the policy.
acl_name	Name of an ACL.
average-data-rate	Configures the QoS average data rate.
average-realtime-rate	Configures the QoS average real-time rate.
burst-data-rate	Configures the QoS burst data rate.
burst-realtime-rate	Configures the QoS burst real-time rate.
qos	Configures a QoS action for the policy.
session-timeout	Configures a session timeout action for the policy.
sleeping-client-timeout	Configures a sleeping client timeout for the policy.
vlan	Configures a VLAN action for the policy.
active	Configures the active hours and days for the policy.
add	Adds active hours and days.
hours	Configures active hours for the policy.
start _time	Start time for the policy.
end _time	End time for the policy.
days	Configures the day on the policy must work.
day	Day of the week, such as **mon, tue, wed, thu, fri, sat, sun**. You can also specify daily or weekdays for the policy to occur daily or on all weekdays.

delete	Deletes active hours and days.
create	Creates a policy.
match	Configures a match criteria for the policy.
device-type	Configures a device type match.
device-type	Device type on which the policy must be applied. You can configure up to 16 devices types for a policy.
eap-type	Configures the Extensible Authentication Protocol (EAP) type as a match criteria.
eap-fast	Configures the EAP type as EAP Flexible Authentication via Secure Tunneling (FAST).
eap-tls	Configures the EAP type as EAP Transport Layer Security (TLS).
leap	Configures the EAP type as Lightweight EAP (LEAP).
peap	Configures the EAP type as Protected EAP (PEAP).
role	Configures the user type or user group for the user.
role_name	User type or user group of the user, for example, student, employee. You can configure only one role per policy.
none	Configures no user type or user group for the user.

Command Default

There is no native profiling policy on the controller.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The maximum number of policies that you can configure is 64.

The following example shows how to configure a role for a policy:

```
(Cisco Controller) > config policy student_policy role student
```

config policy match role

To Configure a role match to a policy, use the **config policy match role**command.

config policy*policy-name***matchrole**{*role-name* | *none*}

Syntax Description

policy-name	Name of the policy.
match	Configures a match to a policy.
role	Configures a role match to a policy.
role-name	Role name to the policy.
none	Name of the Cisco lightweight access point.

Command Default

None.

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to :

```
(Cisco Controller) >config policy match role
```

config port adminmode

To enable or disable the administrative mode for a specific controller port or for all ports, use the **config port adminmode** command.

config port adminmode {**all** | *port*} {**enable** | **disable**}

Syntax Description

all	Configures all ports.
port	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Command Default

Enabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable port 8:

```
(Cisco Controller) > config port adminmode 8 disable
```

The following example shows how to enable all ports:

```
(Cisco Controller) > config port adminmode all enable
```

config port maxspeed

To configure maximum speed for a port, use the **config port maxspeed** command.

config port maxspeed *port* { **1000** | **2500** | **5000** }

Syntax Description

port	Port number
1000	Configures 1 Gbps speed for the port
2500	Configures 2.5 Gbps speed for the port
5000	Configures 5 Gbps speed for the port

Command Default

None

Command History

Release	Modification
8.0	The command was introduced.

Examples

The following example shows how to configure the maximum speed for port 4 to 5 Gbps:

```
(Cisco Controller) > config port maxspeed 4 5000
```

config port linktrap

To enable or disable the up and down link traps for a specific controller port or for all ports, use the **config port linktrap** command.

config port linktrap {**all** | *port*} {**enable** | **disable**}

Syntax Description

all	Configures all ports.
port	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Command Default

The default value for down link traps for a specific controller port or for all ports is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable port 8 traps:

```
(Cisco Controller) > config port linktrap 8 disable
```

The following example shows how to enable all port traps:

```
(Cisco Controller) > config port linktrap all enable
```

config port multicast appliance

To enable or disable the multicast appliance service for a specific controller port or for all ports, use the **config port multicast appliance** commands.

config port multicast appliance {**all** | *port*} {**enable** | **disable**}

Syntax Description

all	Configures all ports.
port	Number of the port.
enable	Enables the specified ports.
disable	Disables the specified ports.

Command Default

The default multicast appliance service for a specific controller port or for all ports is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable multicast appliance service on all ports:

```
(Cisco Controller) > config port multicast appliance all enable
```

The following example shows how to disable multicast appliance service on port 8:

```
(Cisco Controller) > config port multicast appliance 8 disable
```

config prompt

To change the CLI system prompt, use the **config prompt** command.

config prompt *prompt*

Syntax Description

prompt	New CLI system prompt enclosed in double quotes. The prompt can be up to 31 alphanumeric characters and is case sensitive.

Command Default

The system prompt is configured using the startup wizard.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Because the system prompt is a user-defined variable, it is omitted from the rest of this documentation.

The following example shows how to change the CLI system prompt to Cisco 4400:

```
(Cisco Controller) > config prompt "Cisco 4400"
```

config qos average-data-rate

To define the average data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos average-data-rate** command.

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average data rate for the queue bronze.
silver	Specifies the average data rate for the queue silver.
gold	Specifies the average data rate for the queue gold.
platinum	Specifies the average data rate for the queue platinum
per-ssid	Configures the rate limit for an SSID per radio. The c
per-client	Configures the rate limit for each client associated w
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Average data rate for TCP traffic per user. A value be no bandwidth restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the average data rate 0 Kbps for the queue gold per SSID:

```
(Cisco Controller) > config qos average-data-rate gold per ssid downstream 0
```

Related Commands

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

To define the average real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos average-realtime-rate** command.

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the average real-time data rate for the queue bronze.
silver	Specifies the average real-time data rate for the queue silver.
gold	Specifies the average real-time data rate for the queue gold.
platinum	Specifies the average real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Average real-time data rate for UDP traffic per user. A value between 0 restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the average real-time actual rate for queue gold:

```
(Cisco Controller) > config qos average-realtime-rate gold per ssid downstream 10
```

Related Commands

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

To define the peak data rate in Kbps for TCP traffic per user or per service set identifier (SSID), use the **config qos burst-data-rate** command.

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

Syntax Description

bronze	Specifies the peak data rate for the queue bronze.
silver	Specifies the peak data rate for the queue silver.
gold	Specifies the peak data rate for the queue gold.
platinum	Specifies the peak data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Peak data rate for TCP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the peak rate 30000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-data-rate gold per ssid downstream 30000
```

Related Commands

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

To define the burst real-time data rate in Kbps for UDP traffic per user or per service set identifier (SSID), use the **config qos burst-realtime-rate** command.

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} { **per-ssid** | **per-client** } { **downstream** | **upstream** } *rate*

Syntax Description

bronze	Specifies the burst real-time data rate for the queue bronze.
silver	Specifies the burst real-time data rate for the queue silver.
gold	Specifies the burst real-time data rate for the queue gold.
platinum	Specifies the burst real-time data rate for the queue platinum.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Burst real-time data rate for UDP traffic per user. A value between 0 and 51,2000 Kbps (inclusive). A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the queue gold:

```
(Cisco Controller) > config qos burst-realtime-rate gold per ssid downstream  2000
```

Related Commands

config qos average-data-rate

config qos burst-data-rate

config qos average-realtime-rate

config wlan override-rate-limit

config qos description

To change the profile description, use the **config qos description** command.

config qos description {**bronze** | **silver** | **gold** | **platinum**} *description*

Syntax Description

bronze	Specifies the QoS profile description for the queue bronze.
silver	Specifies the QoS profile description for the queue silver.
gold	Specifies the QoS profile description for the queue gold.
platinum	Specifies the QoS profile description for the queue platinum.
description	QoS profile description.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the QoS profile description “description” for the queue gold:

```
(Cisco Controller) > config qos description gold abc
```

Related Commands

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 fastlane

To enable the Fastlane QoS feature on each WLAN, use the **config qos fastlane** command.

config qos fastlane {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables Fastlane QoS on each WLAN.
disable	Disables Fastlane QoS on each WLAN.
wlan-id	WLAN identifier.

Command Default

Fastlane is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
8.3	This command was introduced.

Example

The following example shows how to configure Fastlane QoS on each WLAN:

```
Controller(config)# config qos fastlane enable 1
```

config qos fastlane disable global

To disable the Fastlane QoS feature globally, use the **config qos fastlane disable global** command.

config qos fastlane disable global

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
8.3	This command was introduced.

Usage Guidelines

Fastlane QoS must be disabled on all WLANs before executing this command.

Examples

The following example shows how to disable Fastlane QoS globally for Apple wireless clients:

```
Controller(config)# config qos fastlane disable global
```

config qos max-rf-usage

To specify the maximum percentage of RF usage per access point, use the **config qos max-rf-usage** command.

config qos max-rf-usage {**bronze** | **silver** | **gold** | **platinum**} *usage_percentage*

Syntax Description

bronze	Specifies the maximum percentage of RF usage for the queue bronze.
silver	Specifies the maximum percentage of RF usage for the queue silver.
gold	Specifies the maximum percentage of RF usage for the queue gold.
platinum	Specifies the maximum percentage of RF usage for the queue platinum.
usage-percentage	Maximum percentage of RF usage.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum percentage of RF usage for the queue gold:

```
(Cisco Controller) > config qos max-rf-usage gold 20
```

Related Commands

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

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos dot1p-tag** command.

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *dot1p_tag*

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
dot1p_tag	Dot1p tag value between 1 and 7.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the a QoS 802.1p tag for the queue gold with the dot1p tag value of 5:

```
(Cisco Controller) > config qos dot1p-tag gold 5
```

Related Commands

show qos queue_length all

config qos protocol-type

config qos priority

To define the maximum and default QoS levels for unicast and multicast traffic when you assign a QoS profile to a WLAN, use the **config qos priority** command.

config qos priority {**bronze** | **silver** | **gold** | **platinum**} {*maximum-priority* | *default-unicast-priority* | *default-multicast-priority*}

Syntax Description

bronze	Specifies a Bronze profile of the WLAN.
silver	Specifies a Silver profile of the WLAN.
gold	Specifies a Gold profile of the WLAN.
platinum	Specifies a Platinum profile of the WLAN.
maximum-priority	Maximum QoS priority as one of the following: • besteffort • background • video • voice
default-unicast-priority	Default unicast priority as one of the following: • besteffort • background • video • voice
default-multicast-priority	Default multicast priority as one of the following: • besteffort • background • video • voice

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The maximum priority level should not be lower than the default unicast and multicast priority levels.

The following example shows how to configure the QoS priority for a gold profile of the WLAN with voice as the maximum priority, video as the default unicast priority, and besteffort as the default multicast priority.

```
(Cisco Controller) > config qos priority gold voice video besteffort
```

Related Commands

config qos protocol-type

config qos protocol-type

To define the maximum value (0 to 7) for the priority tag associated with packets that fall within the profile, use the **config qos protocol-type** command.

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} {**none** | *dot1p*}

Syntax Description

bronze	Specifies the QoS 802.1p tag for the queue bronze.
silver	Specifies the QoS 802.1p tag for the queue silver.
gold	Specifies the QoS 802.1p tag for the queue gold.
platinum	Specifies the QoS 802.1p tag for the queue platinum.
none	Specifies when no specific protocol is assigned.
dot1p	Specifies when dot1p type protocol is assigned.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the QoS protocol type silver:

```
(Cisco Controller) > config qos protocol-type silver dot1p
```

Related Commands

show qos queue_length all

config qos dot1p-tag

config qos queue_length

To specify the maximum number of packets that access points keep in their queues, use the **config qos queue_length** command.

config qos queue_length {**bronze** | **silver** | **gold** | **platinum**} *queue_length*

Syntax Description

bronze	Specifies the QoS length for the queue bronze.
silver	Specifies the QoS length for the queue silver.
gold	Specifies the QoS length for the queue gold.
platinum	Specifies the QoS length for the queue platinum.
queue_length	Maximum queue length values (10 to 255).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the QoS length for the queue “gold” with the maximum queue length value as 12:

```
(Cisco Controller) > config qos queue_length gold 12
```

Related Commands

show qos

config qos qosmap

To configure QoS map, use the **config qos qosmap** command.

config qos qosmap {**enable** | **disable** | **default** }

Syntax Description

enable	Enables the QoS map feature.
disable	Disables the QoS map feature.
default	Resets to default QoS map. This resets the QoS map values to 255 (default), and also adds DSCP UP exceptions if not present previously. To clear the DSCP UP values, enter the **config qos qosmap clear-all** command.

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the QoS map.

```
(Cisco Controller) > config qos qosmap enable
```

config qos qosmap up-to-dscp-map

To configure the DSCP range for UP, use the **config qos qosmap** command.

config qos qosmap up-to-dscp-map {*up dscp-default dscp-start dscp-end*}

Syntax Description

up-to-dscp-map	Sets the DSCP range for UP
up	Wireless UP value
dscp-default	Default DSCP value for this UP
dscp-start	The DSCP start range. Range is between 0-63
dscp-end	The DSCP stop range. Range is 0-63

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the DSCP range for UP.

```
(Cisco Controller) > config qos qosmap up-to-dscp-map 2 3 5 20
```

config qos qosmap dscp-to-up-exception

To configure the DSCP exception, use the **config qos qosmap** command.

config qos qosmap dscp-to-up-exception {*dscp up* }

Syntax Description

dscp-to-up-exception	Allows to configure DSCP exception.
dscp	Exception DSCP value for the UP value
up	Links to the Wireless User Priority (UP) value

The following example shows how to configure the DSCP exception:

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 3 1
```

config qos qosmap delete-dscp-exception

To delete a dscp exception, use the **config qos qosmap** command.

config qos qosmap delete-dscp-exception *dscp*

Syntax Description

delete-dscp-exception	Deletes exception for DSCP
dscp	DSCP exception for the UP

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to delete a exception for DSCP.

```
(Cisco Controller) > config qos qosmap delete-dscp-exception 23
```

config qos qosmap clear-all

To delete all the exceptions from the QoS map, use the **config qos qosmap** command.

config qos qosmap clear-all

Syntax Description

clear-all	Deletes all the exceptions

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to clear all the exceptions from the QoS map.

```
(Cisco Controller) > config qos qosmap clear-all
```

config qos qosmap trust dscp upstream

To mark the upstream packets using the client dscp, use the **config qos qosmap** command.

config qos qosmap trust-dscp-upstream {**enable** | **disable** }

Syntax Description

trust-dscp-upstream	Based on the client's DSCP the upstream packets are marked
enable	Enables the upstream packet marking using the client dscp.
disable	Disables the upstream packet marking using the client dscp.

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable client dscp based packet marking.

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
```

Config Commands: r to z

- config radius acct, on page 806
- config radius acct ipsec authentication, on page 809
- config radius acct ipsec disable, on page 810
- config radius acct ipsec enable, on page 811
- config radius acct ipsec encryption, on page 812
- config radius acct ipsec ike, on page 813
- config radius acct mac-delimiter, on page 814
- config radius acct network, on page 815
- config radius acct realm, on page 816
- config radius acct retransmit-timeout, on page 817
- config radius auth, on page 818
- config radius auth callStationIdType, on page 820
- config radius auth framed-mtu, on page 822
- config radius auth IPsec authentication, on page 823
- config radius auth ipsec disable, on page 824
- config radius auth ipsec encryption, on page 825
- config radius auth ipsec ike, on page 826
- config radius auth keywrap, on page 828
- config radius auth mac-delimiter, on page 829
- config radius auth management, on page 830
- config radius auth mgmt-retransmit-timeout, on page 831
- config radius auth network, on page 832
- config radius auth realm, on page 833
- config radius auth retransmit-timeout, on page 834
- config radius auth rfc3576, on page 835
- config radius auth retransmit-timeout, on page 836
- config radius aggressive-failover disabled, on page 837
- config radius backward compatibility, on page 838
- config radius callStationIdCase, on page 839
- config radius callStationIdType, on page 840
- config radius dns, on page 842
- config radius fallback-test, on page 843
- config radius ext-source-ports, on page 845

- config radius acct retransmit-timeout, on page 846
- config radius auth mgmt-retransmit-timeout, on page 847
- config radius auth retransmit-timeout, on page 848
- config radius auth retransmit-timeout, on page 849
- config redundancy interface address peer-service-port, on page 850
- config redundancy mobilitymac, on page 851
- config redundancy mode, on page 852
- config redundancy peer-route, on page 853
- config redundancy timer keep-alive-timer, on page 854
- config redundancy timer peer-search-timer, on page 855
- config redundancy unit, on page 856
- config remote-lan, on page 857
- config remote-lan aaa-override, on page 858
- config remote-lan acl, on page 859
- config remote-lan apgroup, on page 860
- config remote-lan create, on page 861
- config remote-lan custom-web, on page 862
- config remote-lan delete, on page 864
- config remote-lan dhcp_server, on page 865
- config remote-lan exclusionlist, on page 866
- config remote-lan host-mode, on page 867
- config remote-lan interface, on page 868
- config remote-lan ldap, on page 869
- config remote-lan mac-filtering, on page 870
- config remote-lan mab, on page 871
- config remote-lan max-associated-clients, on page 872
- config remote-lan pre-auth, on page 873
- config remote-lan radius_server, on page 874
- config remote-lan security, on page 875
- config remote-lan session-timeout, on page 876
- config remote-lan violation-mode, on page 877
- config remote-lan webauth-exclude, on page 878
- config rf-profile band-select, on page 879
- config rf-profile client-trap-threshold, on page 881
- config rf-profile create, on page 882
- config rf-profile fra client-aware, on page 883
- config rf-profile data-rates, on page 884
- config rf-profile delete, on page 885
- config rf-profile description, on page 886
- config rf-profile fra client-aware, on page 887
- config rf-profile load-balancing, on page 888
- config rf-profile max-clients, on page 889
- config rf-profile multicast data-rate, on page 890
- config rf-profile out-of-box, on page 891
- config rf-profile rx-sop threshold , on page 892
- config rf-profile tx-power-control-thresh-v1, on page 893

- config rf-profile tx-power-control-thresh-v2, on page 894
- config rf-profile tx-power-max, on page 895
- config rf-profile tx-power-min, on page 896
- config rogue ap timeout, on page 897
- config rogue adhoc, on page 898
- config rogue ap classify, on page 901
- config rogue ap friendly, on page 903
- config rogue ap rldp, on page 905
- config rogue ap ssid, on page 907
- config rogue ap timeout, on page 909
- config rogue auto-contain level, on page 910
- config rogue ap valid-client, on page 912
- config rogue client, on page 914
- config rogue containment, on page 916
- config rogue detection, on page 917
- config rogue detection client-threshold, on page 918
- config rogue detection min-rssi, on page 919
- config rogue detection monitor-ap, on page 920
- config rogue detection report-interval, on page 922
- config rogue detection security-level, on page 923
- config rogue detection transient-rogue-interval, on page 924
- config rogue rule, on page 925
- config rogue rule condition ap, on page 929
- config remote-lan session-timeout, on page 931
- config rfid auto-timeout, on page 932
- config rfid status, on page 933
- config rfid timeout, on page 934
- config rogue ap timeout, on page 935
- config route add, on page 936
- config route delete, on page 937
- config serial baudrate, on page 938
- config serial timeout, on page 939
- config service timestamps, on page 940
- config sessions maxsessions, on page 941
- config sessions timeout, on page 942
- config slot, on page 943
- config switchconfig boot-break, on page 944
- config switchconfig fips-prerequisite, on page 945
- config switchconfig ucapl, on page 946
- config switchconfig wlancc, on page 947
- config switchconfig strong-pwd, on page 948
- config switchconfig flowcontrol, on page 951
- config switchconfig mode, on page 952
- config switchconfig secret-obfuscation, on page 953
- config sysname, on page 954
- config snmp community accessmode, on page 955

- config snmp community create, on page 956
- config snmp community delete, on page 957
- config snmp community ipaddr, on page 958
- config snmp community mode, on page 959
- config snmp engineID, on page 960
- config snmp syscontact, on page 961
- config snmp syslocation, on page 962
- config snmp trapreceiver create, on page 963
- config snmp trapreceiver delete, on page 964
- config snmp trapreceiver mode, on page 965
- config snmp v3user create, on page 966
- config snmp v3user delete, on page 968
- config snmp version, on page 969
- config tacacs acct, on page 970
- config tacacs auth, on page 972
- config tacacs auth mgmt-server-timeout, on page 974
- config tacacs dns, on page 975
- config tacacs fallback-test interval, on page 976
- config time manual, on page 977
- config time ntp, on page 978
- config time timezone, on page 981
- config time timezone location, on page 982
- config trapflags 802.11-Security, on page 985
- config trapflags aaa, on page 986
- config trapflags adjchannel-rogueap, on page 987
- config trapflags ap, on page 988
- config trapflags authentication, on page 989
- config trapflags client, on page 990
- config trapflags client max-warning-threshold, on page 991
- config trapflags configsave, on page 992
- config trapflags IPsec, on page 993
- config trapflags linkmode, on page 994
- config trapflags mesh, on page 995
- config trapflags multiusers, on page 996
- config trapflags rfid , on page 997
- config trapflags rogueap, on page 999
- config trapflags rrm-params, on page 1000
- config trapflags rrm-profile, on page 1001
- config trapflags stpmode, on page 1002
- config trapflags strong-pwdcheck, on page 1003
- config trapflags wps, on page 1004
- config tunnel eogre heart-beat, on page 1005
- config tunnel eogre gateway, on page 1006
- config tunnel eogre domain, on page 1007
- config tunnel eogre domain primary, on page 1008
- config tunnel profile, on page 1009

- config tunnel profile_rule, on page 1010
- config tunnel profile_rule-delete, on page 1011
- config tunnel profile eogre-DHCP82, on page 1012
- config tunnel profile eogre-gateway-radius-proxy, on page 1013
- config tunnel profile eogre-gateway-radius-proxy-accounting, on page 1014
- config tunnel profile eogre-DHCP82, on page 1015
- config tunnel profile eogre-DHCP82-circuit-id, on page 1016
- config tunnel profile eogre-DHCP82-delimiter, on page 1017
- config tunnel profile eogre-DHCP82-format, on page 1018
- config tunnel profile eogre-DHCP82-remote-id, on page 1019
- config watchlist add, on page 1020
- config watchlist delete, on page 1021
- config watchlist disable, on page 1022
- config watchlist enable, on page 1023
- config wgb vlan, on page 1024
- config wlan, on page 1025
- config wlan 7920-support, on page 1026
- config wlan 802.11e, on page 1027
- config wlan aaa-override, on page 1028
- config wlan acl, on page 1029
- config wlan apgroup, on page 1030
- config wlan apgroup atf 802.11, on page 1037
- config wlan apgroup atf 802.11 policy, on page 1038
- config wlan apgroup opendns-profile , on page 1039
- config wlan apgroup qinq, on page 1040
- config wlan assisted-roaming, on page 1041
- config wlan atf, on page 1042
- config wlan avc, on page 1043
- config wlan band-select allow, on page 1044
- config wlan broadcast-ssid, on page 1045
- config wlan call-snoop, on page 1046
- config wlan chd, on page 1047
- config wlan ccx aironet-ie, on page 1048
- config wlan channel-scan defer-priority, on page 1049
- config wlan channel-scan defer-time, on page 1050
- config wlan custom-web, on page 1051
- config wlan dhcp_server, on page 1053
- config wlan diag-channel, on page 1054
- config wlan dtim, on page 1055
- config wlan exclusionlist, on page 1056
- config wlan fabric , on page 1057
- config wlan fabric acl, on page 1058
- config wlan fabric avc-policy, on page 1059
- config wlan fabric encap vxlan, on page 1060
- config wlan fabric switch-ip , on page 1061
- config wlan fabric tag, on page 1062

- config wlan fabric vnid , on page 1063
- config wlan flexconnect ap-auth, on page 1064
- config wlan flexconnect central-assoc, on page 1065
- config wlan flexconnect learn-ipaddr, on page 1066
- config wlan flexconnect local-switching, on page 1067
- config wlan flexconnect vlan-central-switching, on page 1069
- config wlan flow, on page 1070
- config wlan hotspot, on page 1071
- config wlan hotspot dot11u, on page 1072
- config wlan hotspot dot11u 3gpp-info, on page 1073
- config wlan hotspot dot11u auth-type, on page 1074
- config wlan hotspot dot11u disable, on page 1075
- config wlan hotspot dot11u domain, on page 1076
- config wlan hotspot dot11u enable, on page 1077
- config wlan hotspot dot11u hessid, on page 1078
- config wlan hotspot dot11u ipaddr-type, on page 1079
- config wlan hotspot dot11u nai-realm, on page 1080
- config wlan hotspot dot11u network-type, on page 1083
- config wlan hotspot dot11u roam-oi , on page 1084
- config wlan hotspot hs2, on page 1085
- config wlan hotspot hs2 domain-id, on page 1088
- config wlan hotspot hs2 osu legacy-ssid, on page 1089
- config wlan hotspot hs2 osu sp create, on page 1090
- config wlan hotspot hs2 osu sp delete, on page 1091
- config wlan hotspot hs2 osu sp icon-file add, on page 1092
- config wlan hotspot hs2 osu sp icon-file delete, on page 1093
- config wlan hotspot hs2 osu sp method add, on page 1094
- config wlan hotspot hs2 osu sp method delete, on page 1095
- config wlan hotspot hs2 osu sp nai add, on page 1096
- config wlan hotspot hs2 osu sp nai delete, on page 1097
- config wlan hotspot hs2 osu sp uri add, on page 1098
- config wlan hotspot hs2 osu sp uri delete, on page 1099
- config wlan hotspot hs2 wan-metrics downlink, on page 1100
- config wlan hotspot hs2 wan-metrics link-status, on page 1101
- config wlan hotspot hs2 wan-metrics lmd, on page 1102
- config wlan hotspot hs2 wan-metrics uplink, on page 1103
- config wlan hotspot msap, on page 1104
- config wlan interface, on page 1105
- config wlan ipv6 acl, on page 1106
- config wlan kts-cac, on page 1107
- config wlan layer2 acl, on page 1108
- config wlan ldap, on page 1109
- config wlan learn-ipaddr-cswlan, on page 1110
- config wlan load-balance, on page 1111
- config wlan lobby-admin-access, on page 1112
- config wlan mac-filtering, on page 1113

- config wlan max-associated-clients, on page 1114
- config wlan max-radio-clients, on page 1115
- config wlan mdns, on page 1116
- config wlan media-stream, on page 1117
- config wlan mfp, on page 1118
- config wlan mobility anchor, on page 1119
- config wlan mobility foreign-map, on page 1120
- config wlan multicast buffer, on page 1121
- config wlan multicast interface, on page 1122
- config wlan mu-mimo, on page 1123
- config wlan nac, on page 1124
- config wlan override-rate-limit, on page 1125
- config wlan opendns-mode, on page 1127
- config wlan opendns-profile, on page 1128
- config wlan passive-client, on page 1129
- config wlan peer-blocking, on page 1130
- config wlan pmipv6 default-realm, on page 1131
- config wlan pmipv6 mobility-type, on page 1132
- config wlan pmipv6 profile_name, on page 1133
- config wlan policy, on page 1134
- config wlan profiling, on page 1135
- config wlan qos, on page 1136
- config wlan radio, on page 1137
- config wlan radius_server acct, on page 1138
- config wlan radius_server acct interim-update, on page 1139
- config wlan radius_server auth, on page 1140
- config wlan radius_server overwrite-interface, on page 1141
- config wlan radius_server realm, on page 1142
- config wlan roamed-voice-client re-anchor, on page 1143
- config wlan security 802.1X, on page 1144
- config wlan security ckip, on page 1146
- config wlan security cond-web-redir, on page 1147
- config wlan security eap-params, on page 1148
- config wlan security eap-passthru, on page 1150
- config wlan security ft, on page 1151
- config wlan security ft over-the-ds, on page 1152
- config wlan security IPsec disable, on page 1153
- config wlan security IPsec enable, on page 1154
- config wlan security IPsec authentication, on page 1155
- config wlan security IPsec encryption, on page 1156
- config wlan security IPsec config, on page 1157
- config wlan security IPsec ike authentication, on page 1158
- config wlan security IPsec ike dh-group, on page 1159
- config wlan security IPsec ike lifetime, on page 1160
- config wlan security IPsec ike phase1, on page 1161
- config wlan security IPsec ike contivity, on page 1162

- config wlan security wpa akm ft, on page 1163
- config wlan security ft, on page 1164
- config wlan security passthru, on page 1165
- config wlan security pmf , on page 1166
- config wlan security sgt, on page 1168
- config wlan security splash-page-web-redir, on page 1169
- config wlan security static-wep-key authentication, on page 1170
- config wlan security static-wep-key disable, on page 1171
- config wlan security static-wep-key enable, on page 1172
- config wlan security static-wep-key encryption, on page 1173
- config wlan security tkip, on page 1174
- config wlan usertimeout, on page 1175
- config wlan security web-auth, on page 1176
- config wlan security web-auth captive-bypass, on page 1178
- config wlan security web-auth qrscan-des-key, on page 1179
- config wlan security web-passthrough acl, on page 1180
- config wlan security web-passthrough disable, on page 1181
- config wlan security web-passthrough email-input, on page 1182
- config wlan security web-passthrough enable, on page 1183
- config wlan security web-passthrough qr-scan, on page 1184
- config wlan security wpa akm 802.1x, on page 1185
- config wlan security wpa akm cckm, on page 1186
- config wlan security wpa akm ft, on page 1187
- config wlan security wpa akm pmf, on page 1188
- config wlan security wpa akm psk, on page 1189
- config wlan security wpa disable, on page 1190
- config wlan security wpa enable, on page 1191
- config wlan security wpa ciphers, on page 1192
- config wlan security wpa gtk-random, on page 1193
- config wlan security wpa osen disable, on page 1194
- config wlan security wpa osen enable, on page 1195
- config wlan security wpa wpa1 disable, on page 1196
- config wlan security wpa wpa1 enable, on page 1197
- config wlan security wpa wpa2 disable, on page 1198
- config wlan security wpa wpa2 enable, on page 1199
- config wlan security wpa wpa2 cache, on page 1200
- config wlan security wpa wpa2 cache sticky, on page 1201
- config wlan security wpa wpa2 ciphers, on page 1202
- config wlan session-timeout, on page 1203
- config wlan sip-cac disassoc-client, on page 1204
- config wlan sip-cac send-486busy, on page 1205
- config wlan static-ip tunneling, on page 1206
- config wlan uapsd compliant client enable, on page 1207
- config wlan uapsd compliant-client disable, on page 1208
- config wlan url-acl, on page 1209
- config wlan user-idle-threshold, on page 1210

- config wlan usertimeout, on page 1211
- config wlan webauth-exclude, on page 1212
- config wlan wgb broadcast-tagging, on page 1213
- config wlan wifidirect, on page 1214
- config wlan wmm, on page 1215
- config wps ap-authentication, on page 1216
- config wps auto-immune, on page 1217
- config wps cids-sensor, on page 1218
- config wps client-exclusion, on page 1220
- config wps mfp, on page 1221
- config wps shun-list re-sync, on page 1222
- config wps signature, on page 1223
- config wps signature frequency, on page 1225
- config wps signature interval, on page 1226
- config wps signature mac-frequency, on page 1227
- config wps signature quiet-time, on page 1228
- config wps signature reset, on page 1229

config radius acct

To configure settings for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct** command.

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*}

Syntax Description

add	Adds a RADIUS accounting server (IPv4 or IPv6).
index	RADIUS server index (1 to 17).
IP addr	RADIUS server IP address (IPv4 or IPv6).
port	RADIUS server's UDP port number for the interface protocols.
ascii	Specifies the RADIUS server's secret type: **ascii**.
hex	Specifies the RADIUS server's secret type: **hex**.
secret	RADIUS server's secret.
enable	Enables a RADIUS accounting server.
disable	Disables a RADIUS accounting server.
delete	Deletes a RADIUS accounting server.
ipsec	Enables or disables IPSec support for an accounting server. **Note** IPSec is not supported for IPv6.
authentication	Configures IPSec Authentication.
hmac-md5	Enables IPSec HMAC-MD5 authentication.
hmac-sha1	Enables IPSec HMAC-SHA1 authentication.
disable	Disables IPSec support for an accounting server.
enable	Enables IPSec support for an accounting server.
encryption	Configures IPSec encryption.
256-aes	Enables IPSec AES-256 encryption.

3des	Enables IPSec 3DES encryption.
aes	Enables IPSec AES-128 encryption.
des	Enables IPSec DES encryption.
ike	Configures Internet Key Exchange (IKE).
auth-mode	Configures IKE authentication method.
pre-shared-key	Pre-shared key for authentication.
certificate	Certificate used for authentication.
dh-group	Configures IKE Diffie-Hellman group.
2048bit-group-14	Configures DH group 14 (2048 bits).
group-1	Configures DH group 1 (768 bits).
group-2	Configures DH group 2 (1024 bits).
group-5	Configures DH group 5 (1536 bits).
lifetime *seconds*	Configures IKE lifetime in seconds. The range is from 1800 to 57600 seconds and the default is 28800.
phase1	Configures IKE phase1 mode.
aggressive	Enables IKE aggressive mode.
main	Enables IKE main mode.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
colon	Sets the delimiter to colon (For example: xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to hyphen (For example: xx-xx-xx-xx-xx-xx).
none	Disables delimiters (For example: xxxxxxxxxx).
single-hyphen	Sets the delimiters to single hyphen (For example: xxxxxx-xxxxxx).
network	Configures a default RADIUS server for network users.
group	Specifies RADIUS server type group.
none	Specifies RADIUS server type none.
provincial	Specifies RADIUS server type provincial.

retransmit-timeout	Changes the default retransmit timeout for the server.
seconds	The number of seconds between retransmissions.
realm	Specifies radius acct realm.
add	Adds radius acct realm.
delete	Deletes radius acct realm.

Command Default

When adding a RADIUS server, the port number defaults to 1813 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a priority 1 RADIUS accounting server at *10.10.10.10* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

The following example shows how to configure a priority 1 RADIUS accounting server at *2001:9:6:40::623* using port *1813* with a login password of *admin*:

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

config radius acct ipsec authentication

To configure IPsec authentication for the Cisco wireless LAN controller, use the **config radius acct ipsec authentication** command.

config radius acct ipsec authentication {**hmac-md5** | **hmac-sha1**} *index*

Syntax Description

hmac-md5	Enables IPsec HMAC-MD5 authentication.
hmac-sha1	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec hmac-md5 authentication service on the RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec authentication hmac-md5 1
```

Related Commands

show radius acct statistics

config radius acct ipsec disable

To disable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec disable** command.

config radius acct ipsec disable *index*

Syntax Description

index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec disable 1
```

Related Commands

show radius acct statistics

config radius acct ipsec enable

To enable IPsec support for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec enable** command.

config radius acct ipsec enable *index*

Syntax Description

index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Examples

The following example shows how to enable the IPsec support for RADIUS accounting server index 1:

```
(Cisco Controller) > config radius acct ipsec enable 1
```

Related Commands

show radius acct statistics

config radius acct ipsec encryption

To configure IPsec encryption for an accounting server for the Cisco wireless LAN controller, use the **config radius acct ipsec encryption** command.

config radius acct ipsec encryption {**3des** | **aes** | **des**} *index*

Syntax Description

256-aes	Enables IPSec AES-256 encryption.
3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES encryption.
des	Enables IPsec DES encryption.
index	RADIUS server index value of between 1 and 17.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec 3DES encryption for RADIUS server index value 3:

```
(Cisco Controller) > config radius acct ipsec encryption 3des 3
```

config radius acct ipsec ike

To configure Internet Key Exchange (IKE) for the controller, use the **config radius acct ipsec ike** command.

config radius acct ipsec ike dh-group {**group-1** | **group-2** | **group-5** | **group-14**} | **lifetime** *seconds* | **phase1** {**aggressive** | **main**}} *index*

Syntax Description

dh-group	Specifies the Dixie-Hellman (DH) group.
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 5 (1024 bits).
group-5	Configures the DH Group 14 (2048 bits).
lifetime	Configures the IKE lifetime.
seconds	IKE lifetime in seconds.
phase1	Configures the IKE phase1 node.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IKE lifetime of 23 seconds for RADIUS server index 1:

```
(Cisco Controller) > config radius acct ipsec ike lifetime 23 1
```

Related Commands

show radius acct statistics

config radius acct mac-delimiter

To specify the delimiter to be used in the MAC addresses that are sent to the RADIUS accounting server, use the **config radius acct mac-delimiter** command.

config radius acct mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets the delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets the delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets the delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default

The default delimiter is a hyphen.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the delimiter hyphen to be used in the MAC addresses that are sent to the RADIUS accounting server for the network users:

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

Related Commands

show radius acct statistics

config radius acct network

To configure a default RADIUS server for network users, use the **config radius acct network** command.

config radius acct network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user's default RADIUS server.
disable	Disables the server as a network user's default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS accounting server for the network users with RADIUS server index1:

```
(Cisco Controller) > config radius acct network 1 enable
```

Related Commands

show radius acct statistics

config radius acct realm

To configure realm on RADIUS accounting server, use the **config radius acct realm** command.

config radius acct realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS accounting server.
delete	Delete realm from RADIUS accounting server.
realm_string	Unique string associated to RADIUS accounting realm.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how add realm to the RADIUS accounting server:

```
(Cisco Controller) > config radius acct realm add 3 test
```

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

config radius auth

To configure settings for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth** command.

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* }

Syntax Description

enable	Enables a RADIUS authentication server.
disable	Disables a RADIUS authentication server.
delete	Deletes a RADIUS authentication server.
index	RADIUS server index. The controller begins the search with 1. The server index range is from 1 to 17.
add	Adds a RADIUS authentication server. See the “Defaults” section.
IP addr	IP address (IPv4 or IPv6) of the RADIUS server.
port	RADIUS server’s UDP port number for the interface protocols.
ascii/hex	Specifies RADIUS server’s secret type: **ascii** or **hex**.
secret	RADIUS server’s secret.
callStationIdType	Configures Called Station Id information sent in RADIUS authentication messages.
framed-mtu	Configures the Framed-MTU for all the RADIUS servers. The framed-mtu range is from 64 to 1300 bytes.
ipsec	Enables or disables IPSEC support for an authentication server. **Note** IPSec is not supported for IPv6.
keywrap	Configures RADIUS keywrap.

ascii/hex	Specifies the input format of the keywrap keys.
kek	Enters the 16-byte key-encryption-key.
mack	Enters the 20-byte message-authenticator-code-key.
mac-delimiter	Configures MAC delimiter for caller station ID and calling station ID.
management	Configures a RADIUS Server for management users.
mgmt-retransmit-timeout	Changes the default management login retransmission timeout for the server.
network	Configures a default RADIUS server for network users.
realm	Configures radius auth realm.
region	Configures RADIUS region property.
retransmit-timeout	Changes the default network login retransmission timeout for the server.
rfc3576	Enables or disables RFC-3576 support for an authentication server.

Command Default

When adding a RADIUS server, the port number defaults to 1812 and the state is **enabled**.

Usage Guidelines

IPSec is not supported for IPv6.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure a priority *3* RADIUS authentication server at *10.10.10.10* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

The following example shows how to configure a priority *3* RADIUS authentication server at *2001:9:6:40::623* using port *1812* with a login password of *admin*:

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

config radius auth callStationIdType

To configure the RADIUS authentication server, use the **config radius auth callStationIdType** command.

config radius auth callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-mac-ssid-ap-group** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.
ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
ap-mac-ssid-ap-group	Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.

Command Default

The MAC address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The **ap-ethmac-only** and **ap-ethmac-ssid** keywords were added to support the access point's Ethernet MAC address. The **ap-label-address** and **ap-label-address-ssid** keywords were added.
8.0	This command supports both IPv4 and IPv6 address formats.
8.3	The **ap-mac-ssid-ap-group** keyword was added.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

config radius auth framed-mtu

To configure the framed-mtu value for all RADIUS servers, use the **config radius auth framed-mtu** command.

config radius auth framed-mtu *mtu*

Syntax Description

mtu	Framed-MTU value range between 64 and 1300 bytes

Note Controller does not use or fragment the framed MTU in the controller. This AV pair that is configurable on the controller is part of the authentication request packet to the RADIUS server and is used to allow the RADIUS server to fragment large packets during events such as 802.1x exchange.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to set the framed-mtu value for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth framed-mtu 500
```

config radius auth IPsec authentication

To configure IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec authentication** command.

config radius auth IPsec authentication {**hmac-md5** | **hmac-sha1**} *index*

Syntax Description

hmac-md5	Enables IPsec HMAC-MD5 authentication.
hmac-shal	Enables IPsec HMAC-SHA1 authentication.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec hmac-md5 support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth IPsec authentication hmac-md5 1
```

Related Commands

show radius acct statistics

config radius auth ipsec disable

To disable IPsec support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth IPsec disable** command.

config radius auth ipsec {**enable** | **disable**} *index*

Syntax Description

enable	Enables the IPsec support for an authentication server.
disable	Disables the IPsec support for an authentication server.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to enable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec enable 1
```

This example shows how to disable the IPsec support for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec disable 1
```

Related Commands

show radius acct statistics

config radius auth ipsec encryption

To configure IPsec encryption support for an authentication server for the Cisco wireless LAN controller, use the **config radius auth ipsec encryption** command.

config radius auth IPsec encryption {**256-aes** | **3des** | **aes** | **des**} *index*

Syntax Description

256-aes	Enables the IPsec 256 AES encryption.
3des	Enables the IPsec 3DES encryption.
aes	Enables the IPsec AES encryption.
des	Enables the IPsec DES encryption.
index	RADIUS server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The keyword 256-aes was added.

The following example shows how to configure IPsec 3dec encryption RADIUS authentication server index 3:

```
(Cisco Controller) > config radius auth ipsec encryption 3des 3
```

Related Commands

show radius acct statistics

config radius auth ipsec ike

To configure Internet Key Exchange (IKE) for the Cisco wireless LAN controller, use the **config radius auth IPsec ike** command.

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*

Syntax Description

auth-mode	Configures the IKE authentication method.
pre-shared-key	Configures the preshared key for IKE authentication method.
index	RADIUS server index between 1 and 17.
ascii	Configures RADIUS IPsec IKE secret in an ASCII format.
hex	Configures RADIUS IPsec IKE secret in a hexadecimal format.
shared-secret	Configures the shared RADIUS IPsec secret.
certificate	Configures the certificate for IKE authentication.
dh-group	Configures the IKE Diffe-Hellman group.
2048bit-group-14	Configures the DH Group14 (2048 bits).
group-1	Configures the DH Group 1 (768 bits).
group-2	Configures the DH Group 2 (1024 bits).
group-5	Configures the DH Group 2 (1024 bits).
lifetime	Configures the IKE lifetime.
seconds	IKE lifetime in seconds. The range is from 1800 to 57600 seconds.
phase1	Configures the IKE phase1 mode.
aggressive	Enables the aggressive mode.
main	Enables the main mode.
index	RADIUS server index.

Command Default

By default, preshared key is used for IPsec sessions and IKE lifetime is 28800 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure IKE lifetime of 23 seconds for RADIUS authentication server index 1:

```
(Cisco Controller) > config radius auth ipsec ike lifetime 23 1
```

Related Commands

show radius acct statistics

config radius auth keywrap

To enable and configure Advanced Encryption Standard (AES) key wrap, which makes the shared secret between the controller and the RADIUS server more secure, use the **config radius auth keywrap** command.

config radius auth keywrap {**enable** | **disable** | **add** {**ascii** | **hex**} *kek mack* | **delete**} *index*

Syntax Description

enable	Enables AES key wrap.
disable	Disables AES key wrap.
add	Configures AES key wrap attributes.
ascii	Configures key wrap in an ASCII format.
hex	Configures key wrap in a hexadecimal format.
kek	16-byte Key Encryption Key (KEK).
mack	20-byte Message Authentication Code Key (MACK).
delete	Deletes AES key wrap attributes.
index	Index of the RADIUS authentication server on which to configure the AES key wrap.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the AES key wrap for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth keywrap enable
```

Related Commands

show radius auth statistics

config radius auth mac-delimiter

To specify a delimiter to be used in the MAC addresses that are sent to the RADIUS authentication server, use the **config radius auth mac-delimiter** command.

config radius auth mac-delimiter {**colon** | **hyphen** | **single-hyphen** | **none**}

Syntax Description

colon	Sets a delimiter to a colon (for example, xx:xx:xx:xx:xx:xx).
hyphen	Sets a delimiter to a hyphen (for example, xx-xx-xx-xx-xx-xx).
single-hyphen	Sets a delimiter to a single hyphen (for example, xxxxxx-xxxxxx).
none	Disables the delimiter (for example, xxxxxxxxxxxx).

Command Default

The default delimiter is a hyphen.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify a delimiter hyphen to be used for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

Related Commands

show radius auth statistics

config radius auth management

To configure a default RADIUS server for management users, use the **config radius auth management** command.

config radius auth management *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a management user's default RADIUS server.
disable	Disables the server as a management user's default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a RADIUS server for management users:

```
(Cisco Controller) > config radius auth management 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth mgmt-retransmit-timeout

config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

Syntax Description

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

Related Commands

config radius auth management

config radius auth network

To configure a default RADIUS server for network users, use the **config radius auth network** command.

config radius auth network *index* {**enable** | **disable**}

Syntax Description

index	RADIUS server index.
enable	Enables the server as a network user default RADIUS server.
disable	Disables the server as a network user default RADIUS server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server for network users:

```
(Cisco Controller) > config radius auth network 1 enable
```

Related Commands

show radius acct statistics

config radius acct network

config radius auth realm

To configure realm on RADIUS authentication server, use the **config radius auth realm** command.

config radius auth realm {**add** | **delete**} *radius_index realm_string*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
add	Add realm to RADIUS authentication server.
delete	Delete realm from RADIUS authentication server.
realm_string	Unique string associated to RADIUS authentication realm.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how add realm to the RADIUS authentication server:

```
(Cisco Controller) > config radius auth realm add 3 test
```

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth rfc3576

To configure RADIUS RFC-3576 support for the authentication server for the controller, use the **config radius auth rfc3576** command.

config radius auth rfc3576 { **enable** | **disable** } *index*

Syntax Description

enable	Enables RFC-3576 support for an authentication server.
disable	Disables RFC-3576 support for an authentication server.
index	RADIUS server index.

Command Default

Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

RFC 3576, which is an extension to the RADIUS protocol, allows dynamic changes to a user session. RFC 3576 includes support for disconnecting users and changing authorizations applicable to a user session. Disconnect messages cause a user session to be terminated immediately; CoA messages modify session authorization attributes such as data filters.

The following example shows how to enable the RADIUS RFC-3576 support for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

Related Commands

show radius auth statistics

show radius summary

show radius rfc3576

config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

Related Commands

show radius auth statistics

show radius summary

config radius aggressive-failover disabled

To configure the controller to mark a RADIUS server as down (not responding) after the server does not reply to three consecutive clients, use the **config radius aggressive-failover disabled** command.

config radius aggressive-failover disabled

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the controller to mark a RADIUS server as down:

```
(Cisco Controller) > config radius aggressive-failover disabled
```

Related Commands

show radius summary

config radius backward compatibility

To configure RADIUS backward compatibility for the controller, use the **config radius backward compatibility** command.

config radius backward compatibility {**enable** | **disable**}

Syntax Description

enable	Enables RADIUS vendor ID backward compatibility.
disable	Disables RADIUS vendor ID backward compatibility.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the RADIUS backward compatibility settings:

```
(Cisco Controller) > config radius backward compatibility disable
```

Related Commands

show radius summary

config radius callStationIdCase

To configure callStationIdCase information sent in RADIUS messages for the controller, use the **config radius callStationIdCase** command.

config radius callStationIdCase { **legacy** | **lower** | **upper** }

Syntax Description

legacy	Configures Call Station IDs for Layer 2 authentication to RADIUS in uppercase.
lower	Configures all Call Station IDs to RADIUS in lowercase.
upper	Configures all Call Station IDs to RADIUS in uppercase.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to send the call station ID in lowercase:

```
(Cisco Controller) > config radius callStationIdCase lower
```

Related Commands

show radius summary

config radius callStationIdType

To configure the Called Station ID type information sent in RADIUS accounting messages for the Cisco wireless LAN controller, use the **config radius callStationIdType** command.

config radius callStationIdType {**ap-ethmac-only** | **ap-ethmac-ssid** | **ap-group-name** | **ap-label-address** | **ap-label-address-ssid** | **ap-location** | **ap-mac-ssid-ap-group** | **ap-macaddr-only** | **ap-macaddr-ssid** | **ap-name** | **ap-name-ssid** | **flex-group-name** | **ipaddr** | **macaddr** | **vlan-id**}

Syntax Description

ipaddr	Configures the Call Station ID type to use the IP address (only Layer 3).
macaddr	Configures the Call Station ID type to use the system's MAC address (Layers 2 and 3).
ap-macaddr-only	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3).
ap-macaddr-ssid	Configures the Call Station ID type to use the access point's MAC address (Layers 2 and 3) in the format *AP MAC address*:*SSID*.
ap-ethmac-only	Configures the Called Station ID type to use the access point's Ethernet MAC address.
ap-ethmac-ssid	Configures the Called Station ID type to use the access point's Ethernet MAC address in the format *AP Ethernet MAC address*:*SSID*.
ap-group-name	Configures the Call Station ID type to use the AP group name. If the AP is not part of any AP group, default-group is taken as the AP group name.
flex-group-name	Configures the Call Station ID type to use the FlexConnect group name. If the FlexConnect AP is not part of any FlexConnect group, the system MAC address is taken as the Call Station ID.
ap-name	Configures the Call Station ID type to use the access point's name.
ap-name-ssid	Configures the Call Station ID type to use the access point's name in the format *AP name*:*SSID*
ap-location	Configures the Call Station ID type to use the access point's location.
ap-mac-ssid-ap-group	Sets Called Station ID type to the format <AP MAC address>:<SSID>:<AP Group>
vlan-id	Configures the Call Station ID type to use the system's VLAN-ID.

Command Default

The IP address of the system.

Usage Guidelines

The controller sends the Called Station ID attribute to the RADIUS server in all authentication and accounting packets. The Called Station ID attribute can be used to classify users to different groups based on the attribute value. The command is applicable only for the Called Station and not for the Calling Station.

You cannot send only the SSID as the Called-Station-ID, you can only combine the SSID with either the access point MAC address or the access point name.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
7.6	The **ap-ethmac-only** and **ap-ethmac-ssid** keywords were added to support the access point's Ethernet MAC address. The **ap-label-address** and **ap-label-address-ssid** keywords were added.
8.0	This command supports both IPv4 and IPv6 address formats.
8.3	The **ap-mac-ssid-ap-group** keyword was added.

The following example shows how to configure the call station ID type to use the IP address:

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

The following example shows how to configure the call station ID type to use the system's MAC address:

```
(Cisco Controller) > config radius callStationIdType macaddr
```

The following example shows how to configure the call station ID type to use the access point's MAC address:

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

config radius dns

To retrieve the RADIUS IP information from a DNS server, use the **config radius dns** command.

config radius dns { **global** *port* { *ascii* | *hex* } *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable** }

Syntax Description

global	Configures the global port and secret to retrieve the RADIUS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	RADIUS server login secret.
query	Configures the fully qualified domain name (FQDN) of the RADIUS server and DNS timeout.
url	FQDN of the RADIUS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the controller waits for, in days, before timing out the request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the RADIUS DNS feature. By default, this feature is disabled.
enable	Enables the controller to retrieve the RADIUS IP information from a DNS server. When you enable a DNS query, the static configurations are overridden, that is, the DNS list overrides the static AAA list.

Command Default

You cannot configure the global port and secret to retrieve the RADIUS IP information.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret.

The following example shows how to enable the RADIUS DNS feature on the controller:

```
(Cisco Controller) > config radius dns enable
```

config radius fallback-test

To configure the RADIUS server fallback behavior, use the **config radius fallback-test** command.

config radius fallback-test mode {**off** | **passive** | **active**} | **username** *username*} | {**interval** *interval*}

Syntax Description

mode	Specifies the mode.
off	Disables RADIUS server fallback.
passive	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers without using extraneous probe messages. The controller ignores all inactive servers for a time period and retries later when a RADIUS message needs to be sent.
active	Causes the controller to revert to a preferable server (with a lower server index) from the available backup servers by using RADIUS probe messages to proactively determine whether a server that has been marked inactive is back online. The controller ignores all inactive servers for all active RADIUS requests.
username	Specifies the username.
username	Username. The username can be up to 16 alphanumeric characters.
interval	Specifies the probe interval value.
interval	Probe interval. The range is 180 to 3600.

Command Default

The default probe interval is 300.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the RADIUS accounting server fallback behavior:

```
(Cisco Controller) > config radius fallback-test mode off
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers without using the extraneous probe messages:

```
(Cisco Controller) > config radius fallback-test mode passive
```

The following example shows how to configure the controller to revert to a preferable server from the available backup servers by using RADIUS probe messages:

```
(Cisco Controller) > config radius fallback-test mode active
```

Related Commands

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

config radius ext-source-ports

To configure support for extended source ports in the RADIUS servers, use the **config radius ext-source-ports** command.

config radius ext-source-ports { **enable** | **disable** }

Syntax Description

enable	Enables Radius source port support.
disable	Disables Radius source port support.

Command Default

None

Command Modes

Config

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the extended source ports in the RADIUS servers:

```
config radius ext-source-ports enable
```

config radius acct retransmit-timeout

To change the default transmission timeout for a RADIUS accounting server for the Cisco wireless LAN controller, use the **config radius acct retransmit-timeout** command.

config radius acct retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure retransmission timeout value 5 seconds between the retransmission:

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

Related Commands

show radius acct statistics

config radius auth mgmt-retransmit-timeout

To configure a default RADIUS server retransmission timeout for management users, use the **config radius auth mgmt-retransmit-timeout** command.

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

Syntax Description

index	RADIUS server index.
retransmit-timeout	Timeout value. The range is from 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default RADIUS server retransmission timeout for management users:

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

Related Commands

config radius auth management

config radius auth retransmit-timeout

To change a default transmission timeout for a RADIUS authentication server for the Cisco wireless LAN controller, use the **config radius auth retransmit-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Number of seconds (from 2 to 30) between retransmissions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a retransmission timeout of 5 seconds for a RADIUS authentication server:

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

Related Commands

show radius auth statistics

config radius auth retransmit-timeout

To configure a retransmission timeout value for a RADIUS accounting server, use the **config radius auth server-timeout** command.

config radius auth retransmit-timeout *index timeout*

Syntax Description

index	RADIUS server index.
timeout	Timeout value. The range is from 2 to 30 seconds.

Command Default

The default timeout is 2 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a server timeout value of 2 seconds for RADIUS authentication server index 10:

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

Related Commands

show radius auth statistics

show radius summary

config redundancy interface address peer-service-port

To configure the service port IP and netmask of the peer or standby controller, use the **config redundancy interface address peer-service-port** command.

config redundancy interface address peer-service-port *ip_address netmask*

Syntax Description

ip_address	IP address of the peer service port.
netmask	Netmask of the peer service port.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will loose these configurations if you change the mode from HA to non-HA and vice-versa.

The following example shows how to configure the service port IP and netmask of the peer or standby controller:

```
(Cisco Controller) >config redundancy interface address peer-service-port 11.22.44.55
```

config redundancy mobilitymac

To configure the High Availability mobility MAC address to be used as an identifier, use the **config redundancy mobilitymac** command.

config redundancy mobilitymac *mac_address*

Syntax Description

mac_address	MAC address that is an identifier for the active and standby controller pair.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

From Release 8.0.132.0 onwards, mobility MAC configuration is no longer present in the uploaded configuration. Therefore, if you download this configuration file back to the controller, you must add the **config redundancy mobilitymac** *mac_address*command in the config file before download.

Examples

The following example shows how to configure the High Availability mobility MAC address:

```
(Cisco Controller) >config redundancy mobilitymac ff:ff:ff:ff:ff:ff
```

config redundancy mode

To enable or disable redundancy or High Availability (HA), use the **config redundancy mode** command.

config redundancy mode {**sso** | **none**}

Syntax Description

sso	Enables a stateful switch over (SSO) or hot standby redundancy mode.
none	Disables redundancy mode.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must configure local and peer redundancy management IP addresses before you configure redundancy.

The following example shows how to enable redundancy:

```
(Cisco Controller) >config redundancy mode sso
```

config redundancy peer-route

To configure the route configurations of the peer or standby controller, use the **config redundancy peer-route** command.

config redundancy peer-route {**add** | **delete**} *network_ip_address netmask gateway*

Syntax Description

add	Adds a network route.
delete	Deletes a network route specific to standby controller.
network_ip_address	Network IP address.
netmask	Subnet mask of the network.
gateway	IP address of the gateway for the route network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure this command only from the Active controller. For the HA feature, the service port configurations are made per controller. You will lose these configurations if you change the mode from HA to non-HA and vice-versa.

The following example shows how to configure route configurations of a peer or standby controller.

```
(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

To configure the keep-alive timeout value, use the **config redundancy timer keep-alive-timer** command.

config redundancy timer keep-alive-timer *milliseconds*

Syntax Description

milliseconds	Keep-alive timeout value in milliseconds. The range is from 100 to 400 milliseconds.

Command Default

The default keep-alive timeout value is 100 milliseconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the keep-alive timeout value:

```
(Cisco Controller) >config redundancy timer keep-alive-timer 200
```

config redundancy timer peer-search-timer

To configure the peer search timer, use the **config redundancy timer peer-search-timer** command.

config redundancy timer peer-search-timer *seconds*

Syntax Description

seconds	Value of the peer search timer in seconds. The range is from 60 to 180 secs.

Command Default

The default value of the peer search timer is 120 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command to configure the boot up role negotiation timeout value in seconds.

The following example shows how to configure the redundancy peer search timer:

```
(Cisco Controller) >config redundancy timer peer-search-timer 100
```

config redundancy unit

To configure a controller as a primary or secondary controller, use the **config redundancy unit** command.

config redundancy unit { **primary** | **secondary** }

Syntax Description

primary	Configures the controller as the primary controller.
secondary	Configures the controller as the secondary controller.

Command Default

The default state is as the primary controller.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you configure a controller as the secondary controller, it becomes the High Availability Stackable Unit (SKU) without any valid AP licenses.

The following example shows how to configure a controller as the primary controller:

```
(Cisco Controller) >config redundancy unit primary
```

config remote-lan

To configure a remote LAN, use the **config remote-lan** command.

config remote-lan {**enable** | **disable**} {*remote-lan-id* | **all**}

Syntax Description

enable	Enables a remote LAN.
disable	Disables a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
all	Configures all wireless LANs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a remote LAN with ID 2:

```
(Cisco Controller) >config remote-lan enable 2
```

config remote-lan aaa-override

To configure user policy override through AAA on a remote LAN, use the **config remote-lan aaa-override** command.

config remote-lan aaa-override {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables user policy override through AAA on a remote LAN.
disable	Disables user policy override through AAA on a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable user policy override through AAA on a remote LAN where the remote LAN ID is 2:

```
(Cisco Controller) >config remote-lan aaa-override enable 2
```

config remote-lan acl

To specify an access control list (ACL) for a remote LAN, use the **config remote-lan acl** command.

config remote-lan acl *remote-lan-id acl_name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
acl_name	ACL name. **Note** Use the **show acl summary** command to know the ACLs available.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify ACL1 for a remote LAN whose ID is 2:

```
(Cisco Controller) >config remote-lan acl 2 ACL1
```

config remote-lan apgroup

To add an access point (AP) group to remote LAN IEEE 802.1X, use the **config remote-lan apgroup** command.

config remote-lan apgroup add *apgroup-name description*

Syntax Description

add	Creates a new AP group.
apgroup-name	Name of an AP group to configure.
description	(Optional) Description of the AP group.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

Example

The following example shows how to add an AP group to remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan apgroup add testap
```

config remote-lan create

To configure a new remote LAN connection, use the **config remote-lan create** command.

config remote-lan create *remote-lan-id name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
name	Remote LAN name. Valid values are up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a new remote LAN, MyRemoteLAN, with the LAN ID as 3:

```
(Cisco Controller) >config remote-lan create 3 MyRemoteLAN
```

config remote-lan custom-web

To configure web authentication for a remote LAN, use the **config remote-lan custom-web** command.

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*

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
URL	Web authentication URL for the Login page.
global	Configures the global status for the remote LAN.
enable	Enables the global status for the remote LAN.
disable	Disables the global status for the remote LAN.
login-page	Configures a login page.
page-name	Login page name.
none	Configures no login page.
logout-page	Configures a logout page.
none	Configures no logout page.
webauth-type	Configures the web authentication type for the remote LAN.
internal	Displays the default login page.
customized	Displays a downloaded login page.
external	Displays a login page that is on an external server.
name	Remote LAN name. Valid values are up to 32 alphanumeric characters.
remote-lan-id	Remote LAN identifier. Valid values are from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Follow these guidelines when you use the **config remote-lan custom-web** command:

- When you configure the external Web-Auth URL, do the following:
  - Ensure that Web-Auth or Web-Passthrough Security is in enabled state. To enable Web-Auth, use the **config remote-lan security web-auth enable** command. To enable Web-Passthrough, use the **config remote-lan security web-passthrough enable** command.

- Ensure that the global status of the remote LAN is in disabled state. To enable the global status of the remote LAN, use the **config remote-lan custom-web global disable** command.
- Ensure that the remote LAN is in disabled state. To disable a remote LAN, use the **config remote-lan disable** command.

- When you configure the Web-Auth type for the remote LAN, do the following:
  - When you configure a customized login page, ensure that you have a login page configured. To configure a login page, use the **config remote-lan custom-web login-page** command.
  - When you configure an external login page, ensure that you have configured preauthentication ACL for external web authentication to function.

The following example shows how to configure an external web authentication URL for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 3
```

The following example shows how to enable the global status of a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web global enable 3
```

The following example shows how to configure the login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web login-page custompage1 3
```

The following example shows how to configure a web authentication type with the default login page for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan custom-web webauth-type internal 3
```

config remote-lan delete

To delete a remote LAN connection, use the **config remote-lan delete** command.

config remote-lan delete *remote-lan-id*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan delete 3
```

config remote-lan dhcp_server

To configure a dynamic host configuration protocol (DHCP) server for a remote LAN, use the **config remote-lan dhcp_server** command.

config remote-lan dhcp_server *remote-lan-id ip_address*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
ip_addr	IPv4 address of the override DHCP server.

Command Default

0.0.0.0 is set as the default interface value.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to configure a DHCP server for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan dhcp_server 3 209.165.200.225
```

Related Commands

show remote-lan

config remote-lan exclusionlist

To configure the exclusion list timeout on a remote LAN, use the **config remote-lan exclusionlist** command.

config remote-lan exclusionlist *remote-lan-id* {*seconds* | **disabled** | **enabled**}

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Exclusion list timeout in seconds. A value of 0 requires an administrator override.
disabled	Disables exclusion listing.
enabled	Enables exclusion listing.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the exclusion list timeout to 20 seconds on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan exclusionlist 3 20
```

config remote-lan host-mode

To configure a host mode for remote LAN IEEE 802.1X, use the **config remote-lan host-mode** command.

config remote-lan host-mode {**singlehost** | **multihost** } *remote-lan-id*

Syntax Description

singlehost	Configures the remote LAN single-host mode.
multihost	Configures the remote LAN multi-host mode.
remote-lan-id	WLAN identifier. The range is from 1 to 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to configure the host mode as single for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan host-mode singlehost 1
```

config remote-lan interface

To configure an interface for a remote LAN, use the **config remote-lan interface** command.

config remote-lan interface *remote-lan-id interface_name*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
interface_name	Interface name. **Note** Interface name should not be in upper case characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface myinterface for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan interface 3 myinterface
```

config remote-lan ldap

To configure a remote LAN's LDAP servers, use the **config remote-lan ldap** command.

config remote-lan ldap {**add** | **delete**} *remote-lan-id index*

Syntax Description

add	Adds a link to a configured LDAP server (maximum of three).
delete	Deletes a link to a configured LDAP server.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
index	LDAP server index.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an LDAP server with the index number 10 for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan ldap add 3 10
```

config remote-lan mac-filtering

To configure MAC filtering on a remote LAN, use the **config remote-lan mac-filtering** command.

config remote-lan mac-filtering {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables MAC filtering on a remote LAN.
disable	Disables MAC filtering on a remote LAN.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.

Command Default

MAC filtering on a remote LAN is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable MAC filtering on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan mac-filtering disable 3
```

config remote-lan mab

To configure MAC Authentication Bypass (MAB) authentication support for AP Port LAN clients, use the **config remote-lan mab** command.

config remote-lan mab {**enable** | **disable**} *remote-lan-id*

Syntax Description

enable	Enables MAB authentication support.
disable	Disables MAB authentication support.
remote-lan-id	WLAN Identifier. The valid range is between 1 and 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to enable MAB authentication support for AP Port LAN clients:

```
(Cisco Controller) >config remote-lan mab enable 8
```

config remote-lan max-associated-clients

To configure the maximum number of client connections on a remote LAN, use the **config remote-lan max-associated-clients** command.

config remote-lan max-associated-clients *remote-lan-id max-clients*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
max-clients	Configures the maximum number of client connections on a remote LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure 10 client connections on a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan max-associated-clients 3 10
```

config remote-lan pre-auth

To configure a preauthentication VLAN for RLAN IEEE 802.1X, use the **config remote-lan pre-auth** command.

config remote-lan pre-auth {**enable** | **disable**} *remote-lan-id* **vlan** *vlan-id*

Syntax Description

enable	Enables RLAN preauthentication.
disable	Disables RLAN preauthentication.
remote-lan-id	WLAN identifier. The range is from 1 to 512.
vlan	Configures preauthentication VLAN for RLAN IEEE 802.1X.
vlan-id	Remote LAN preauthentication VLAN identifier.

Command Default

None

Command Modes

(Controller Configuration)

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to enable preauthentication VLAN for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan pre-auth enable 1 vlan vlan1
```

config remote-lan radius_server

To configure the RADIUS servers on a remote LAN, use the **config remote-lan radius_server** command.

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*

Syntax Description

acct	Configures a RADIUS accounting server.
add	Adds a link to a configured RADIUS server.
delete	Deletes a link to a configured RADIUS server.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
server-index	RADIUS server index.
enable	Enables RADIUS accounting for this remote LAN.
disable	Disables RADIUS accounting for this remote LAN.
interim-update	Enables RADIUS accounting for this remote LAN.
interval	Accounting interim interval. The range is from 180 to 3600 seconds.
enable	Enables accounting interim update.
disable	Disables accounting interim update.
auth	Configures a RADIUS authentication server.
enable	Enables RADIUS authentication for this remote LAN.
disable	Disables RADIUS authentication for this remote LAN.
overwrite-interface	Configures a RADIUS dynamic interface for the remote LAN.
enable	Enables a RADIUS dynamic interface for the remote LAN.
disable	Disables a RADIUS dynamic interface for the remote LAN.

Command Default

The interim update interval is set to 600 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for a remote LAN with ID 3:

```
(Cisco Controller) >config remote-lan radius_server acct enable 3
```

config remote-lan security

To configure security policy for a remote LAN, use the **config remote-lan security** command.

config remote-lan security {{**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *remote-lan-id* | {**web-passthrough** {**enable** | **disable** | **acl** | **email-input**} *remote-lan-id*}}

Syntax Description

web-auth	Specifies web authentication.
enable	Enables the web authentication settings.
disable	Disables the web authentication settings.
acl	Configures an access control list.
server-precedence	Configures the authentication server precedence order for web authentication users.
remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
email-input	Configures the web captive portal using an e-mail address.
web-passthrough	Specifies the web captive portal with no authentication required.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.4	The **802.1X** keyword was added.

The following example shows how to configure the security web authentication policy for remote LAN ID 1:

```
(Cisco Controller) >config remote-lan security web-auth enable 1
```

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config remote-lan violation-mode

To configure the violation mode for remote LAN IEEE 802.1X, use the **config remote-lan violation-mode** command.

config remote-lan violation-mode {**protect** | **replace** | **shutdown**} *remote-lan-id*

Syntax Description

protect	Configures the remote LAN protect mode.
replace	Configures the remote LAN replace mode.
shutdown	Configures the remote LAN shutdown mode.
remote-lan-id	WLAN identifier. The range is from 1 to 512.

Command Default

None

Command Modes

Controller Configuration

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

Example

The following example shows how to configure the violation mode as protect for remote LAN IEEE 802.1X:

```
(Cisco Controller) > config remote-lan violation-mode protect 1
```

config remote-lan webauth-exclude

To configure web authentication exclusion on a remote LAN, use the **config remote-lan webauth-exclude** command.

config remote-lan webauth-exclude *remote-lan-id* {**enable** | **disable**}

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
enable	Enables web authentication exclusion on the remote LAN.
disable	Disables web authentication exclusion on the remote LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable web authentication exclusion on a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan webauth-exclude 1 enable
```

config rf-profile band-select

To configure the RF profile band selection parameters, use the **config rf-profile band-select** command.

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*

Syntax Description

client-rssi	Configures the client Received Signal Strength Indicator (RSSI) threshold for the RF profile.
rssi	Minimum RSSI for a client to respond to a probe. The range is from -20 to -90 dBm.
cycle-count	Configures the probe cycle count for the RF profile. The cycle count sets the number of suppression cycles for a new client.
cycles	Value of the cycle count. The range is from 1 to 10.
cycle-threshold	Configures the time threshold for a new scanning RF Profile band select cycle period. This setting determines the time threshold during which new probe requests from a client come in a new scanning cycle.
value	Value of the cycle threshold for the RF profile. The range is from 1 to 1000 milliseconds.
expire	Configures the expiration time of clients for band select.
dual-band	Configures the expiration time for pruning previously known dual-band clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for a dual band. The range is from 10 to 300 seconds.
suppression	Configures the expiration time for pruning previously known 802.11b/g clients. After this time elapses, clients become new and are subject to probe response suppression.
value	Value for suppression. The range is from 10 to 200 seconds.
probe-response	Configures the probe response for a RF profile.
enable	Enables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
disable	Disables probe response suppression on clients operating in the 2.4-GHz band for a RF profile.
profile name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The default value for client RSSI is –80 dBm.

The default cycle count is 2.

The default cycle threshold is 200 milliseconds.

The default value for dual-band expiration is 60 seconds.

The default value for suppression expiration is 20 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-Ghz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to configure the client RSSI:

```
(Cisco Controller) >config rf-profile band-select client-rssi -70
```

config rf-profile client-trap-threshold

To configure the threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller, use the **config rf-profile client-trap-threshold** command.

config rf-profile client-trap-threshold *threshold profile_name*

Syntax Description

threshold	Threshold value of the number of clients that associate with an access point, after which an SNMP trap is sent to the controller. The range is from 0 to 200. Traps are disabled if the threshold value is configured as zero.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold value of the number of clients that associate with an access point:

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

config rf-profile create

To create a RF profile, use the **config rf-profile create** command.

config rf-profile create {**802.11a** | **802.11b/g**} *profile-name*

Syntax Description

802.11a	Configures the RF profile for the 2.4GHz band.
802.11b/g	Configures the RF profile for the 5GHz band.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to create a new RF profile:

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

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*}

Syntax Description

client-reset	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
percent	Utilization percentage value ranges from 0 to 100. The default is 5%.
rf-profile-name	Name of the RF Profile.
client-select	Configures the RF profile utilization threshold for radio to switch to 5GHz.
percent	Utilization percentage value ranges from 0 to 100. The default is 50%.
disable	Disables the RF profile client-aware FRA feature.
enable	Enables the RF profile client-aware FRA feature.

Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile data-rates

To configure the data rate on a RF profile, use the **config rf-profile data-rates** command.

config rf-profile data-rates {**802.11a** | **802.11b** } {**disabled** | **mandatory** | **supported**} *data-rate profile-name*

Syntax Description

802.11a	Specifies 802.11a as the radio policy of the RF profile.
802.11b	Specifies 802.11b as the radio policy of the RF profile.
disabled	Disables a rate.
mandatory	Sets a rate to mandatory.
supported	Sets a rate to supported.
data-rate	802.11 operational rates, which are 1*, 2*, 5.5*, 6, 9, 11*, 12, 18, 24, 36, 48 and 54, where * denotes 802.11b only rates.
profile-name	Name of the RF profile.

Command Default

Default data rates for RF profiles are derived from the controller system defaults, the global data rate configurations. For example, if the RF profile's radio policy is mapped to 802.11a then the global 802.11a data rates are copied into the RF profiles at the time of creation.

The data rates set with this command are negotiated between the client and the Cisco wireless LAN controller. If the data rate is set to mandatory, the client must support it in order to use the network. If a data rate is set as supported by the Cisco wireless LAN controller, any associated client that also supports that rate may communicate with the Cisco lightweight access point using that rate. It is not required that a client is able to use all the rates marked supported in order to associate.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the 802.11b transmission of an RF profile at a mandatory rate at 12 Mbps:

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroup1
```

config rf-profile delete

To delete a RF profile, use the **config rf-profile delete** command.

config rf-profile delete *profile-name*

Syntax Description

profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a RF profile:

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

config rf-profile description

To provide a description to a RF profile, use the **config rf-profile description** command.

config rf-profile description *description profile-name*

Syntax Description

description	Description of the RF profile.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a description to a RF profile:

```
(Cisco Controller) >config rf-profile description This is a demo desciption RFGroup1
```

config rf-profile fra client-aware

To configure the RF profile client-aware FRA feature, use the **config rf-profile fra client-aware** command.

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*}

Syntax Description

client-reset	Configures the RF profile AP utilization threshold for radio to switch back to Monitor mode.
percent	Utilization percentage value ranges from 0 to 100. The default is 5%.
rf-profile-name	Name of the RF Profile.
client-select	Configures the RF profile utilization threshold for radio to switch to 5GHz.
percent	Utilization percentage value ranges from 0 to 100. The default is 50%.
disable	Disables the RF profile client-aware FRA feature.
enable	Enables the RF profile client-aware FRA feature.

Command Default

The default percent value for client-select and client-reset is 50% and 5% respectively.

Command History

Release	Modification
8.5	This command was introduced.

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch back from 5GHz client-serving role to Monitor mode:

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

The following example shows how to configure the RF profile utilization threshold for redundant dual-band radios to switch from Monitor mode to 5GHz client-serving role:

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

The following example shows how to disable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

The following example shows how to enable the RF profile client-aware FRA feature:

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile load-balancing

To configure load balancing on an RF profile, use the **config rf-profile load-balancing** command.

config rf-profile load-balancing {**window** *clients* | **denial** *value*} *profile_name*

Syntax Description

window	Configures the client window for load balancing of an RF profile.
clients	Client window size that limits the number of client associations with an access point. The range is from 0 to 20. The default value is 5. The window size is part of the algorithm that determines whether an access point is too heavily loaded to accept more client associations: *load-balancing window + client associations on AP with lightest load = load-balancing threshold* Access points with more client associations than this threshold are considered busy, and clients can associate only to access points with client counts lower than the threshold. This window also helps to disassociate sticky clients.
denial	Configures the client denial count for load balancing of an RF profile.
value	Maximum number of association denials during load balancing. The range is from 1 to 10. The default value is 3. When a client tries to associate on a wireless network, it sends an association request to the access point. If the access point is overloaded and load balancing is enabled on the controller, the access point sends a denial to the association request. If there are no other access points in the range of the client, the client tries to associate the same access point again. After the maximum denial count is reached, the client is able to associate. Association attempts on an access point from any client before associating any AP is called a sequence of association. The default is 3.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client window size for an RF profile:

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

config rf-profile max-clients

To configure the maximum number of client connections per access point of an RF profile, use the **config rf-profile max-clients** commands.

config rf-profile max-clients *clients*

Syntax Description

clients	Maximum number of client connections per access point of an RF profile. The range is from 1 to 200.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command to configure the maximum number of clients on access points that are in client dense areas, or serving high bandwidth video or mission critical voice applications.

The following example shows how to set the maximum number of clients at 50:

```
(Cisco Controller) >config rf-profile max-clients 50
```

config rf-profile multicast data-rate

To configure the minimum RF profile multicast data rate, use the **config rf-profile multicast data-rate** command.

config rf-profile multicast data-rate *value profile_name*

Syntax Description

value	Minimum RF profile multicast data rate. The options are 6, 9, 12, 18, 24, 36, 48, 54. Enter 0 to specify that access points will dynamically adjust the data rate.
profile_name	Name of the RF profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

The minimum RF profile multicast data rate is 0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the multicast data rate for an RF profile:

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

config rf-profile out-of-box

To create an out-of-box AP group consisting of newly installed access points, use the **config rf-profile out-of-box** command.

config rf-profile out-of-box {**enable** | **disable**}

Syntax Description

enable	Enables the creation of an out-of-box AP group. When you enable this command, the following occurs: • Newly installed access points that are part of the default AP group will be part of the out-of-box AP group and their radios will be switched off, which eliminates any RF instability caused by the new access points. • All access points that do not have a group name become part of the out-of-box AP group. • Special RF profiles are created per 802.11 band. These RF profiles have default-settings for all the existing RF parameters and additional new configurations.
disable	Disables the out-of-box AP group. When you disable this feature, only the subscription of new APs to the out-of-box AP group stops. All APs that are subscribed to the out-of-box AP group remain in this AP group. You can move APs to the default group or a custom AP group upon network convergence.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When an out-of-box AP associates with the controller for the first time, it will be redirected to a special AP group and the RF profiles applicable to this AP Group will control the radio admin state configuration of the AP. You can move APs to the default group or a custom group upon network convergence.

The following example shows how to enable the creation of an out-of-box AP group:

```
(Cisco Controller) >config rf-profile out-of-box enable
```

config rf-profile rx-sop threshold

To configure high, medium or low Rx SOP threshold values for each 802.11 band, use the **config rf-profile rx-sop threshold** command.

config rf-profile rx-sop threshold {**high** | **medium** | **low** | **auto**} *profile_name*

Syntax Description

high	Configures the high Rx SOP threshold value for an RF profile.
medium	Configures the medium Rx SOP threshold value for an RF profile.
low	Configures the low Rx SOP threshold value for an RF profile.
auto	Configures an auto Rx SOP threshold value for an RF profile. When you choose auto, the access point determines the best Rx SOP threshold value.
profile_name	RF profile on which the Rx SOP threshold value will be configured.

Command Default

The default Rx SOP threshold option is auto.

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to configure the high Rx SOP threshold value on an RF profile:

```
(Cisco Controller) > config 802.11 rx-sop threshold high T1a
```

config rf-profile tx-power-control-thresh-v1

To configure Transmit Power Control version1 (TPCv1) to an RF profile, use the **config rf-profile tx-power-control-thresh-v1** command.

config rf-profile tx-power-control-thresh-v1 *tpc-threshold profile_name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv1 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```

config rf-profile tx-power-control-thresh-v2

To configure Transmit Power Control version 2 (TPCv2) to an RF profile, use the **config rf-profile tx-power-control-thresh-v2** command.

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

Syntax Description

tpc-threshold	TPC threshold.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure TPCv2 on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

config rf-profile tx-power-max

To configure maximum auto-rf to an RF profile, use the **config rf-profile tx-power-max** command.

config rf-profile *tx-power-max profile-name*

Syntax Description

tx-power-max	Maximum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-max on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

config rf-profile tx-power-min

To configure minimum auto-rf to an RF profile, use the **config rf-profile tx-power-min** command.

config rf-profile tx-power-min *tx-power-min profile-name*

Syntax Description

tx-power-min	Minimum auto-rf tx power.
profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure tx-power-min on an RF profile:

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

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

To globally or individually configure the status of an Independent Basic Service Set (IBSS or *ad-hoc*) rogue access point, use the **config rogue adhoc** command.

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*}

Syntax Description

enable	Globally enables detection and reporting of ad-hoc rogues.
disable	Globally disables detection and reporting of ad-hoc rogues.
external	Configure external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
rogue_MAC	MAC address of the ad-hoc rogue access point.
alert	Generates an SMNP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action.
all	Enables alerts for all ad-hoc rogue access points.
auto-contain	Contains all wired ad-hoc rogues detected by the controller.
monitor_ap	(Optional) IP address of the ad-hoc rogue access point.
contain	Contains the offending device so that its signals no longer interfere with authorized clients.
1234_aps	Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).
delete	Deletes ad-hoc rogue access points.
all	Deletes all ad-hoc rogue access points.
mac-address	Deletes ad-hoc rogue access point with the specified MAC address.
mac-address	MAC address of the ad-hoc rogue access point.

classify	Configures ad-hoc rogue access point classification.
friendly state	Classifies ad-hoc rogue access points as friendly.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
malicious state	Classifies ad-hoc rogue access points as malicious.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.
contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
unclassified state	Classifies ad-hoc rogue access points as unclassified.

Command Default

The default for this command is **enabled** and is set to **alert**. The default for auto-containment is **disabled**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses RLDP to determine if the rogue is attached to your wired network.

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

Enter the **auto-contain** command with the *monitor_ap* argument to monitor the rogue access point without containing it. Enter the **auto-contain** command without the optional *monitor_ap* to automatically contain all wired ad-hoc rogues detected by the controller.

The following example shows how to enable the detection and reporting of ad-hoc rogues:

```
(Cisco Controller) > config rogue adhoc enable
```

The following example shows how to enable alerts for all ad-hoc rogue access points:

```
(Cisco Controller) > config rogue adhoc alert all
```

The following example shows how to classify an ad-hoc rogue access point as friendly and configure external state on it:

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

Related Commands

config rogue auto-contain level

show rogue ignore-list

show rogue rule detailed

show rogue rule summary

config rogue ap classify

To classify the status of a rogue access point, use the **config rogue ap classify** command.

config rogue ap classify {**friendly state** {**internal** | **external**} *ap_mac* }

config rogue ap classify {**malicious** | **unclassified**} **state** {**alert** | **contain**} *ap_mac*

Syntax Description

friendly	Classifies a rogue access point as friendly.
state	Specifies a response to classification.
internal	Configures the controller to trust this rogue access point.
external	Configures the controller to acknowledge the presence of this access point.
ap_mac	MAC address of the rogue access point.
malicious	Classifies a rogue access point as potentially malicious.
unclassified	Classifies a rogue access point as unknown.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.

Command Default

These commands are disabled by default. Therefore, all unknown access points are categorized as **unclassified** by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A rogue access point cannot be moved to the unclassified class if its current state is contain.

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to classify a rogue access point as friendly and can be trusted:

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as malicious and to send an alert:

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

The following example shows how to classify a rogue access point as unclassified and to contain it:

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

Related Commands

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

To add a new friendly access point entry to the friendly MAC address list, or delete an existing friendly access point entry from the list, use the **config rogue ap friendly** command.

config rogue ap friendly {**add** | **delete**} *ap_mac*

Syntax Description

add	Adds this rogue access point from the friendly MAC address list.
delete	Deletes this rogue access point from the friendly MAC address list.
ap_mac	MAC address of the rogue access point that you want to add or delete.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a new friendly access point with MAC address 11:11:11:11:11:11 to the friendly MAC address list.

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

Related Commands

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

To enable, disable, or initiate the Rogue Location Discovery Protocol (RLDP), use the **config rogue ap rldp** command.

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

Syntax Description

alarm-only	When entered without the optional argument *monitor_ap_only*, enables RLDP on all access points.
auto-contain	When entered without the optional argument *monitor_ap_only*, automatically contains all rogue access points.
monitor_ap_only	(Optional) RLDP is enabled (when used with **alarm-only** keyword), or automatically contained (when used with **auto-contain** keyword) is enabled only on the designated monitor access point.
initiate	Initiates RLDP on a specific rogue access point.
rogue_mac_address	MAC address of specific rogue access point.
disable	Disables RLDP on all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: “Using this feature may have legal consequences. Do you want to continue?” The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party’s network could have legal consequences.

The following example shows how to enable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

The following example shows how to enable RLDP on monitor-mode access point ap_1:

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

The following example shows how to start RLDP on the rogue access point with MAC address 123.456.789.000:

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

The following example shows how to disable RLDP on all access points:

```
(Cisco Controller) > config rogue ap rldp disable
```

Related Commands

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

To generate an alarm only, or to automatically contain a rogue access point that is advertising your network's service set identifier (SSID), use the **config rogue ap ssid** command.

config rogue ap ssid {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be advertising your network's SSID.
auto-contain	Automatically contains the rogue access point that is advertising your network's SSID.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is advertising your network's SSID:

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

Related Commands

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

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

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

To configure rogue the auto-containment level, use the **config rogue auto-contain level** command.

config rogue auto-contain level *level* [**monitor_ap_only**]

Syntax Description

level	Rogue auto-containment level in the range of 1 to 4. You can enter a value of 0 to enable the controller to automatically select the number of APs used for auto containment. The controller chooses the required number of APs based on the RSSI for effective containment. **Note** Up to four APs can be used to auto-contain when a rogue AP is moved to contained state through any of the auto-containment policies.
monitor_ap_only	(Optional) Configures auto-containment using only monitor AP mode.

Command Default

The default auto-containment level is 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller continuously monitors all nearby access points and automatically discovers and collects information on rogue access points and clients. When the controller discovers a rogue access point, it uses any of the configured auto-containment policies to start autocontainment. The policies for initiating autocontainment are rogue on wire (detected through RLDP or rogue detector AP), rogue using managed SSID, Valid client on Rogue AP, and AdHoc Rogue.

This table lists the RSSI value associated with each containment level.

Table 7: RSSI Associated with Each Containment Level

Auto-containment Level	RSSI
1	0 to –55 dBm
2	–75 to –55 dBm
3	–85 to –75 dBm
4	Less than –85 dBm

Note RLDP is not supported for use with Cisco autonomous rogue access points. These access points drop the DHCP Discover request sent by the RLDP client. Also, RLDP is not supported if the rogue access point channel requires dynamic frequency selection (DFS).

When you enter any of the containment commands, the following warning appears:

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

The 2.4-GHz and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to configure the auto-contain level to 3:

```
(Cisco Controller) > config rogue auto-contain level 3
```

Related Commands

config rogue adhoc

show rogue adhoc summary

show rogue client summary

show rogue ignore-list

show rogue rule summary

config rogue ap valid-client

To generate an alarm only, or to automatically contain a rogue access point to which a trusted client is associated, use the **config rogue ap valid-client** command.

config rogue ap valid-client {**alarm** | **auto-contain**}

Syntax Description

alarm	Generates only an alarm when a rogue access point is discovered to be associated with a valid client.
auto-contain	Automatically contains a rogue access point to which a trusted client is associated.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enter any of the containment commands, the following warning appears: "Using this feature may have legal consequences. Do you want to continue?" The 2.4- and 5-GHz frequencies in the Industrial, Scientific, and Medical (ISM) band are open to the public and can be used without a license. As such, containing devices on another party's network could have legal consequences.

The following example shows how to automatically contain a rogue access point that is associated with a valid client:

```
(Cisco Controller) > config rogue ap valid-client auto-contain
```

Related Commands

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

To configure rogue clients, use the **config rogue client** command.

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**} } }

Syntax Description

aaa	Configures AAA server or local database to validate whether rogue clients are valid clients. The default is disabled.
enable	Enables the AAA server or local database to check rogue client MAC addresses for validity.
disable	Disables the AAA server or local database to check rogue client MAC addresses for validity.
alert	Configures the controller to forward an immediate alert to the system administrator for further action.
ap_mac	Access point MAC address.
contain	Configures the controller to contain the offending device so that its signals no longer interfere with authorized clients.
client_mac	MAC address of the rogue client.
delete	Deletes the rogue client.
state	Deletes the rogue clients according to their state.
alert	Deletes the rogue clients in alert state.
any	Deletes the rogue clients in any state.
contained	Deletes all rogue clients that are in contained state.
contained-pending	Deletes all rogue clients that are in contained pending state.
all	Deletes all rogue clients.
mac-address	Deletes a rogue client with the configured MAC address.
mse	Validates if the rogue clients are valid clients using MSE. The default is disabled.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot validate rogue clients against MSE and AAA at the same time.

The following example shows how to enable the AAA server or local database to check MAC addresses:

```
(Cisco Controller) > config rogue client aaa enable
```

The following example shows how to disable the AAA server or local database from checking MAC addresses:

```
(Cisco Controller) > config rogue client aaa disable
```

Related Commands

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

To configure rogue containment, use the **config rogue containment** command.

config rogue containment {**flexconnect** | **auto-rate**} {**enable** | **disable**}

Syntax Description

flexconnect	Configures rogue containment for standalone FlexConnect APs.
auto-rate	Configures automatic rate selection for rogue containment.
enable	Enables the rogue containment.
disable	Disables the rogue containment.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

The following table lists the rogue containment automatic rate selection details.

Table 8: Rogue Containment Automatic Rate Selection

RSSI (dBm)	802.11b/g Tx Rate (Mbps)	802.11a Tx Rate (Mbps)
–74	1	6
–70	2	12
–55	5.5	12
< –40	5.5	18

The following example shows how to enable automatic rate selection for rogue containment:

```
(Cisco Controller) > config rogue containment auto-rate enable
```

config rogue detection

To enable or disable rogue detection, use the **config rogue detection** command.

Note If an AP itself is configured with the keyword **all**, the **all access points** case takes precedence over the AP that is with the keyword **all**.

config rogue detection {**enable** | **disable**} {*cisco_ap* | **all**}

Syntax Description

enable	Enables rogue detection on this access point.
disable	Disables rogue detection on this access point.
cisco_ap	Cisco access point.
all	Specifies all access points.

Command Default

The default rogue detection value is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Rogue detection is enabled by default for all access points joined to the controller except for OfficeExtend access points. OfficeExtend access points are deployed in a home environment and are likely to detect a large number of rogue devices.

The following example shows how to enable rogue detection on the access point Cisco_AP:

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

Related Commands

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

To configure the rogue client threshold for access points, use the **config rogue detection client-threshold** command.

config rogue detection client-threshold *value*

Syntax Description

value	Threshold rogue client count on an access point after which a trap is sent from the controller. The range is from 1 to 256. Enter 0 to disable the feature.

Command Default

The default rogue client threshold is 0.

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to configure the rogue client threshold:

```
(Cisco Controller) >config rogue detection client-threshold 200
```

config rogue detection min-rssi

To configure the minimum Received Signal Strength Indicator (RSSI) value at which APs can detect rogues and create a rogue entry in the controller, use the **config rogue detection min-rssi** command.

config rogue detection min-rssi *rssi-in-dBm*

Syntax Description

rssi-in-dBm	Minimum RSSI value. The valid range is from –70 dBm to –128 dBm, and the default value is –128 dBm.

Command Default

The default RSSI value to detect rogues in APs is -128 dBm.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This feature is applicable to all the AP modes.

There can be many rogues with very weak RSSI values that do not provide any valuable information in rogue analysis. Therefore, you can use this option to filter rogues by specifying the minimum RSSI value at which APs should detect rogues.

The following example shows how to configure the minimum RSSI value:

```
(Cisco Controller) > config rogue detection min-rssi –80
```

Related Commands

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

To configure the rogue report interval for all monitor mode Cisco APs, use the **config rogue detection monitor-ap** command.

config rogue detection monitor-ap {**report-interval** | **transient-rogue-interval**} *time-in-seconds*

Syntax Description

report-interval	Specifies the interval at which rogue reports are sent.
transient-rogue-interval	Specifies the interval at which rogues are consistently scanned for by APs after the first time the rogues are scanned.
time-in-seconds	Time in seconds. The valid range is as follows: • 10 to 300 for **report-interval** • 120 to 1800 for **transient-rogue-interval**

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This feature is applicable to APs that are in monitor mode only.

Using the transient interval values, you can control the time interval at which APs should scan for rogues. APs can also filter the rogues based on their transient interval values.

This feature has the following advantages:

- Rogue reports from APs to the controller are shorter.
- Transient rogue entries are avoided in the controller.
- Unnecessary memory allocation for transient rogues are avoided.

The following example shows how to configure the rogue report interval to 60 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

The following example shows how to configure the transient rogue interval to 300 seconds:

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

Related Commands

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

To configure the rogue detection report interval, use the **config rogue detection report-interval** command.

config rogue detection report-interval *time*

Syntax Description

time	Time interval, in seconds, at which the access points send the rogue detection report to the controller. The range is from 10 to 300.

Command Default

The default rogue detection report interval is 10 seconds.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This feature is applicable only to the access points that are in the monitor mode.

The following example shows how to configure the rogue detection report interval:

```
(Cisco Controller) >config rogue detection report-interval 60
```

config rogue detection security-level

To configure the rogue detection security level, use the **config rogue detection security-level** command.

config rogue detection security-level {**critical** | **custom** | **high** | **low**}

Syntax Description

critical	Configures the rogue detection security level to critical.
custom	Configures the rogue detection security level to custom, and allows you to configure the rogue policy parameters.
high	Configures the rogue detection security level to high. This security level configures basic rogue detection and auto containment for medium-scale or less critical deployments. The Rogue Location Discovery Protocol (RLDP) is disabled for this security level.
low	Configures the rogue detection security level to low. This security level configures basic rogue detection for small-scale deployments. Auto containment is not supported for this security level.

Command Default

The default rogue detection security level is custom.

Command History

Release	Modification
7.5	This command was introduced.

The following example shows how to configure the rogue detection security level to high:

```
(Cisco Controller) > config rogue detection security-level high
```

config rogue detection transient-rogue-interval

To configure the rogue-detection transient interval, use the **config rogue detection transient-rogue-interval** command.

config rogue detection transient-rogue-interval *time*

Syntax Description

time	Time interval, in seconds, at which a rogue should be consistently scanned by the access point after the rogue is scanned for the first time. The range is from 120 to 1800.

Command Default

The default rogue-detection transient interval for each security level is as follows:

- Low—120 seconds
- High—300 seconds
- Critical—600 seconds

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This feature applies only to the access points that are in the monitor mode.

After the rogue is scanned consistently, updates are sent periodically to the controller. The access points filter the active transient rogues for a very short period and are then silent.

The following example shows how to configure the rogue detection transient interval:

```
(Cisco Controller) > config rogue detection transient-rogue-interval 200
```

config rogue rule

To add and configure rogue classification rules, use the **config rogue rule** command.

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*}

Syntax Description

add ap priority	Adds a rule with match any criteria and the priority that you specify.
priority	Priority of this rule within the list of rules.
classify	Specifies the classification of a rule.
custom	Classifies devices matching the rule as custom.
severity-score	Custom classification severity score of the rule. The range is from 1 to 100.
classification-name	Custom classification name. The name can be up to 32 case-sensitive, alphanumeric characters.
friendly	Classifies a rule as friendly.
malicious	Classifies a rule as malicious.
notify	Configures type of notification upon rule match.
all	Notifies the controller and a trap receiver such as Cisco Prime Infrastructure.
global	Notifies only a trap receiver such as Cisco Prime Infrastructure.
local	Notifies only the controller.
none	Notifies neither the controller nor a trap receiver such as Cisco Prime Infrastructure.
state	Configures state of the rogue access point after a rule match.
alert	Configures alert state on the rogue access point that is not in the neighbor list or in the user configured friendly MAC list. The controller forwards an immediate alert to the system administrator for further action.

contain	Configures contain state on the rogue access point. Controller contains the offending device so that its signals no longer interfere with authorized clients.
delete	Configures delete state on the rogue access point.
external	Configures external state on the rogue access point that is outside the network and poses no threat to WLAN security. The controller acknowledges the presence of this rogue access point.
internal	Configures alert state on rogue access point that is inside the network and poses no threat to WLAN security. The controller trusts this rogue access point.
rule_name	Rule to which the command applies, or the name of a new rule.
condition ap	Specifies the conditions for a rule that the rogue access point must meet.
set	Adds conditions to a rule that the rogue access point must meet.
delete	Removes conditions to a rule that the rogue access point must meet.
condition_type	Type of the condition to be configured. The condition types are listed below: • client-count—Requires that a minimum number of clients be associated to a rogue access point. The valid range is 1 to 10 (inclusive). • duration—Requires that a rogue access point be detected for a minimum period of time. The valid range is 0 to 3600 seconds (inclusive). • managed-ssid—Requires that a rogue access point's SSID be known to the controller. • no-encryption—Requires that a rogue access point's advertised WLAN does not have encryption enabled. • rssi—Requires that a rogue access point have a minimum RSSI value. The range is from –95 to –50 dBm (inclusive). • ssid—Requires that a rogue access point have a specific SSID. • substring-ssid—Requires that a rogue access point have a substring of a user-configured SSID.

condition_value	Value of the condition. This value is dependent upon the condition_type. For instance, if the condition type is ssid, then the condition value is either the SSID name or all.
enable	Enables all rules or a single specific rule.
delete	Deletes all rules or a single specific rule.
disable	Deletes all rules or a single specific rule.
match	Specifies whether a detected rogue access point must meet all or any of the conditions specified by the rule in order for the rule to be matched and the rogue access point to adopt the classification type of the rule.
all	Specifies all rules defined.
any	Specifies any rule meeting certain criteria.
priority	Changes the priority of a specific rule and shifts others in the list accordingly.

Command Default

No rogue rules are configured.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

For your changes to be effective, you must enable the rule. You can configure up to 64 rules.

Reclassification of rogue APs according to the RSSI condition of the rogue rule occurs only when the RSSI changes more than +/- 2 dBm of the configured RSSI value. Manual and automatic classification override custom rogue rules. Rules are applied to manually changed rogues if their class type changes to unclassified and state changes to alert. Adhoc rogues are classified and do not go to the pending state. You can have up to 50 classification types.

The following example shows how to create a rule called rule_1 with a priority of 1 and a classification as friendly.

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

The following example shows how to enable rule_1.

```
(Cisco Controller) > config rogue rule enable rule_1
```

The following example shows how to change the priority of the last command.

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

The following example shows how to change the classification of the last command.

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

The following example shows how to disable the last command.

```
(Cisco Controller) > config rogue rule disable rule_1
```

The following example shows how to delete SSID_2 from the user-configured SSID list in rule-5.

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

The following example shows how to create a custom rogue rule.

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

config rogue rule condition ap

To configure a condition of a rogue rule for rogue access points, use the **config rogue rule condition ap** command.

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*

Syntax Description

set	Configures conditions to a rule that the rogue access point must meet.
client-count	Enables a minimum number of clients to be associated to the rogue access point.
count	Minimum number of clients to be associated to the rogue access point. The range is from 1 to 10 (inclusive). For example, if the number of clients associated to a rogue access point is greater than or equal to the configured value, the access point is classified as malicious.
duration	Enables a rogue access point to be detected for a minimum period of time.
time	Minimum time period, in seconds, to detect the rogue access point. The range is from 0 to 3600.
managed-ssid	Enables a rogue access point's SSID to be known to the controller.
no-encryption	Enables a rogue access point's advertised WLAN to not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it.
rssi	Enables a rogue access point to have a minimum Received Signal Strength Indicator (RSSI) value.
rssi	Minimum RSSI value, in dBm, required for the access point. The range is from –95 to –50 (inclusive). For example, if the rogue access point has an RSSI that is greater than the configured value, the access point is classified as malicious.
ssid	Enables a rogue access point have a specific SSID.
ssid	SSID of the rogue access point.
substring-ssid	Enables a rogue access point to have a substring of a user-configured SSID.
substring-ssid	Substring of a user-configured SSID. For example, if you have an SSID as ABCDE, you can specify the substring as ABCD or ABC. You can classify multiple SSIDs with matching patterns.
delete	Removes the conditions to a rule that a rogue access point must comply with.
all	Deletes all the rogue rule conditions.
rule_name	Rogue rule to which the command applies.

Command Default

The default value for RSSI is 0 dBm.

The default value for duration is 0 seconds.

The default value for client count is 0.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure up to 25 SSIDs per rogue rule. You can configure up to 25 SSID substrings per rogue rule.

The following example shows how to configure the RSSI rogue rule condition:

```
(Cisco Controller) > config rogue rule condition ap set rssi -50
```

config remote-lan session-timeout

To configure client session timeout, use the **config remote-lan session-timeout** command.

config remote-lan session-timeout *remote-lan-id seconds*

Syntax Description

remote-lan-id	Remote LAN identifier. Valid values are between 1 and 512.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client session timeout to 6000 seconds for a remote LAN with ID 1:

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config rfid auto-timeout

To configure an automatic timeout of radio frequency identification (RFID) tags, use the **config rfid auto-timeout** command.

config rfid auto-timeout {**enable** | **disable**}

Syntax Description

enable	Enables an automatic timeout.
disable	Disables an automatic timeout.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an automatic timeout of RFID tags:

```
(Cisco Controller) > config rfid auto-timeout enable
```

Related Commands

show rfid summary

config rfid status

config rfid timeout

config rfid status

To configure radio frequency identification (RFID) tag data tracking, use the **config rfid status** command.

config rfid status {**enable** | **disable**}

Syntax Description

enable	Enables RFID tag tracking.
disable	Enables RFID tag tracking.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure RFID tag tracking settings:

```
(Cisco Controller) > config rfid status enable
```

Related Commands

show rfid summary

config rfid auto-timeout

config rfid timeout

config rfid timeout

To configure a static radio frequency identification (RFID) tag data timeout, use the **config rfid timeout** command.

config rfid timeout *seconds*

Syntax Description

seconds	Timeout in seconds (from 60 to 7200).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a static RFID tag data timeout of 60 seconds:

```
(Cisco Controller) > config rfid timeout 60
```

Related Commands

show rfid summary

config rfid statistics

config rogue ap timeout

To specify the number of seconds after which the rogue access point and client entries expire and are removed from the list, use the **config rogue ap timeout** command.

config rogue ap timeout *seconds*

Syntax Description

seconds	Value of 240 to 3600 seconds (inclusive), with a default value of 1200 seconds.

Command Default

The default number of seconds after which the rogue access point and client entries expire is 1200 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set an expiration time for entries in the rogue access point and client list to 2400 seconds:

```
(Cisco Controller) > config rogue ap timeout 2400
```

Related Commands

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

To configure a network route from the service port to a dedicated workstation IP address range, use the **config route add** command.

config route add *ip_address netmask gateway*

Syntax Description

ip_address	Network IP address.
netmask	Subnet mask for the network.
gateway	IP address of the gateway for the route network.

Command Default

None

Usage Guidelines

As on release 7.6, *IP_address* supports only IPv4 addresses.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6. This command supports only IPv4 address format.

The following example shows how to configure a network route to a dedicated workstation IP address 10.1.1.0, subnet mask 255.255.255.0, and gateway 10.1.1.1:

```
(Cisco Controller) > config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config route delete

To remove a network route from the service port, use the **config route delete** command.

config route delete *ip_address*

Syntax Description

ip_address	Network IP address.

Command Default

None

Usage Guidelines

As on release 7.6, *IP_address* supports only IPv4 addresses.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv6 address format.

The following example shows how to delete a route from the network IP address 10.1.1.0:

```
(Cisco Controller) > config route delete 10.1.1.0
```

config serial baudrate

To set the serial port baud rate, use the **config serial baudrate** command.

config serial baudrate {**1200** | **2400** | **4800** | **9600** | **19200** | **38400** | **57600**}

Syntax Description

1200	Specifies the supported connection speeds to 1200.
2400	Specifies the supported connection speeds to 2400.
4800	Specifies the supported connection speeds to 4800.
9600	Specifies the supported connection speeds to 9600.
19200	Specifies the supported connection speeds to 19200.
38400	Specifies the supported connection speeds to 38400.
57600	Specifies the supported connection speeds to 57600.

Command Default

The default serial port baud rate is 9600.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a serial baud rate with the default connection speed of 9600:

```
(Cisco Controller) > config serial baudrate 9600
```

config serial timeout

To set the timeout of a serial port session, use the **config serial timeout** command.

config serial timeout *minutes*

Syntax Description

minutes	Timeout in minutes from 0 to 160. A value of 0 indicates no timeout.

Command Default

0 (no timeout)

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to set the timeout for a serial connection to the front of the Cisco wireless LAN controller from 0 to 160 minutes where 0 is no timeout.

The following example shows how to configure the timeout of a serial port session to 10 minutes:

```
(Cisco Controller) > config serial timeout 10
```

config service timestamps

To enable or disable time stamps in message logs, use the **config service timestamps** command.

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

Syntax Description

debug	Configures time stamps in debug messages.
log	Configures time stamps in log messages.
datetime	Specifies to time-stamp message logs with the standard date and time.
disable	Specifies to prevent message logs being time-stamped.

Command Default

By default, the time stamps in message logs are disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure time-stamp message logs with the standard date and time:

```
(Cisco Controller) > config service timestamps log datetime
```

The following example shows how to prevent message logs being time-stamped:

```
(Cisco Controller) > config service timestamps debug disable
```

Related Commands

show logging

config sessions maxsessions

To configure the number of Telnet CLI sessions allowed by the controller, use the **config sessions maxsessions** command.

config sessions maxsessions *session_num*

Syntax Description

session_num	Number of sessions from 0 to 5.

Command Default

The default number of Telnet CLI sessions allowed by the controller is 5.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Up to five sessions are possible while a setting of zero prohibits any Telnet CLI sessions.

The following example shows how to configure the number of allowed CLI sessions to 2:

```
(Cisco Controller) > config sessions maxsessions 2
```

Related Commands

show sessions

config sessions timeout

To configure the inactivity timeout for Telnet CLI sessions, use the **config sessions timeout** command.

config sessions timeout *timeout*

Syntax Description

timeout	Timeout of Telnet session in minutes (from 0 to 160). A value of 0 indicates no timeout.

Command Default

The default inactivity timeout for Telnet CLI sessions is 5 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the inactivity timeout for Telnet sessions to 20 minutes:

```
(Cisco Controller) > config sessions timeout 20
```

Related Commands

show sessions

config slot

To configure various slot parameters, use the **config slot** command.

config slot *slot_id* {**enable** | **disable** | **channel ap** | **chan_width** | **txpower ap** | **antenna extAntGain** *antenna_gain* | **rts**} *cisco_ap*

Syntax Description

slot_id	Slot downlink radio to which the channel is assigned. Beginning in Release 7.5 and later releases, you can configure 802.11a on slot 1 and 802.11ac on slot 2.
enable	Enables the slot.
disable	Disables the slot.
channel	Configures the channel for the slot.
ap	Configures one 802.11a Cisco access point.
chan_width	Configures channel width for the slot.
txpower	Configures Tx power for the slot.
antenna	Configures the 802.11a antenna.
extAntGain	Configures the 802.11a external antenna gain.
antenna_gain	External antenna gain value in .5 dBi units (such as 2.5 dBi = 5).
rts	Configures RTS/CTS for an access point.
cisco_ap	Name of the Cisco access point on which the channel is configured.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable slot 3 for the access point abc:

```
(Cisco Controller) >config slot 3 enable abc
```

The following example shows how to configure RTS for the access point abc:

```
(Cisco Controller) >config slot 2 rts abc
```

config switchconfig boot-break

To enable or disable the breaking into boot prompt by pressing the Esc key at system startup, use the **config switchconfig boot-break** command.

config switchconfig boot-break {**enable** | **disable**}

Syntax Description

enable	Enables the breaking into boot prompt by pressing the Esc key at system startup.
disable	Disables the breaking into boot prompt by pressing the Esc key at system startup.

Command Default

By default, the breaking into boot prompt by pressing the Esc key at system startup is disabled.

Usage Guidelines

You must enable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode before enabling or disabling the breaking into boot prompt.

The following example shows how to enable the breaking into boot prompt by pressing the Esc key at system startup:

```
(Cisco Controller) > config switchconfig boot-break enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig strong-pwd

config switchconfig fips-prerequisite

To enable or disable the features that are prerequisites for the Federal Information Processing Standard (FIPS) mode, use the **config switchconfig fips-prerequisite** command.

config switchconfig fips-prerequisite {**enable** | **disable**}

Syntax Description

enable	Enables the features that are prerequisites for the FIPS mode.
disable	Disables the features that are prerequisites for the FIPS mode.

Command Default

By default, the features that are prerequisites for the FIPS mode are disabled.

Usage Guidelines

You must configure the FIPS authorization secret before you can enable or disable the FIPS prerequisite features.

The following example shows how to enable the features that are prerequisites for the FIPS mode:

```
(Cisco Controller) > config switchconfig fips-prerequisite enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig boot-break

config switchconfig strong-pwd

config switchconfig ucapl

To configure US Department of Defense (DoD) Unified Capabilities Approved Product List (APL) certification on the controller, use the **config switchconfig wlancc** command.

config switchconfig ucapl {**enable** | **disable**}

Syntax Description

enable	Enables UCAPL on the controller.
disable	Disables UCAPL on the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable UCAPL on the controller:

```
(Cisco Controller) > config switchconfig ucapl enable
```

config switchconfig wlancc

To configure WLAN Common Criteria (CC) on the controller, use the **config switchconfig wlancc** command.

config switchconfig wlancc {**enable** | **disable**}

Syntax Description

enable	Enables WLAN CC on the controller.
disable	Disables WLAN CC on the controller.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable WLAN CC on the controller:

```
(Cisco Controller) > config switchconfig wlancc enable
```

config switchconfig strong-pwd

To enable or disable your controller to check the strength of newly created passwords, use the **config switchconfig strong-pwd** command.

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** }

Syntax Description

case-check	Checks at least three combinations: lowercase characters, uppercase characters, digits, or special characters.
consecutive-check	Checks the occurrence of the same character three times.
default-check	Checks for default values or use of their variants.
username-check	Checks whether the username is specified or not.
position-check	Checks whether the password has a four-character change from the old password.
case-digit-check	Checks whether the password has all the four combinations: lower, upper, digits, or special characters.
minimum	Checks whether the password has a minimum number of upper case and lower case characters, digits, or special characters.
upper-case	Checks whether the password has a minimum number of upper case characters.
lower-case	Checks whether the password has a minimum number of lower case characters.
digits	Checks whether the password has a minimum number of digits.
special-chars	Checks whether the password has a minimum number of special characters.
min-length	Configures the minimum length for the password.
password_length	Minimum length for the password. The range is from 3 to 24 case-sensitive characters.

lockout	Configures the lockout feature for a management user or Simple Network Management Protocol version 3 (SNMPv3) user.
mgmtuser	Locks out a management user when the number of successive failed attempts exceed the management user lockout attempts.
snmpv3user	Locks out a SNMPv3 user when the number of successive failed attempts exceeds the SNMPv3 user lockout attempts.
time	Configures the time duration after the lockout attempts when the management user or SNMPv3 user is locked.
attempts	Configures the number of successive incorrect password attempts after which the management user or SNMPv3 user is locked.
lifetime	Configures the number of days before the management user or SNMPv3 user requires a change of password due to the age of the password.
mgmtuser	Configures the number of days before the management user requires a change of password due to the password age.
snmpv3user	Configures the number of days before the SNMPv3 user requires a change of password due to the age of the password.
lifetime	Number of days before the management user or SNMPv3 user requir*lifetime*s a change of password due to the age of the password.
all-checks	Checks all the cases.
enable	Enables a strong password check for the access point and controller.
disable	Disables a strong password check for the access point and controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Strong Password Check feature:

```
(Cisco Controller) > config switchconfig strong-pwd case-check enable
```

Related Commands

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig boot-break

config switchconfig flowcontrol

To enable or disable 802.3x flow control, use the **config switchconfig flowcontrol** command.

config switchconfig flowcontrol {**enable** | **disable**}

Syntax Description

enable	Enables 802.3x flow control.
disable	Disables 802.3x flow control.

Command Default

By default, 802.3x flow control is disabled.

The following example shows how to enable 802.3x flow control on Cisco wireless LAN controller parameters:

```
(Cisco Controller) > config switchconfig flowcontrol enable
```

Related Commands

show switchconfig

config switchconfig mode

To configure Lightweight Access Port Protocol (LWAPP) transport mode for Layer 2 or Layer 3, use the **config switchconfig mode** command.

config switchconfig mode {**L2** | **L3**}

Syntax Description

L2	Specifies Layer 2 as the transport mode.
L3	Specifies Layer 3 as the transport mode.

Command Default

The default transport mode is L3.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure LWAPP transport mode to Layer 3:

```
(Cisco Controller) > config switchconfig mode L3
```

Related Commands

show switchconfig

config switchconfig secret-obfuscation

To enable or disable secret obfuscation, use the **config switchconfig secret-obfuscation** command.

config switchconfig secret-obfuscation {**enable** | **disable**}

Syntax Description

enable	Enables secret obfuscation.
disable	Disables secret obfuscation.

Command Default

Secrets and user passwords are obfuscated in the exported XML configuration file.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To keep the secret contents of your configuration file secure, do not disable secret obfuscation. To further enhance the security of the configuration file, enable configuration file encryption.

The following example shows how to enable secret obfuscation:

```
(Cisco Controller) > config switchconfig secret-obfuscation enable
```

Related Commands

show switchconfig

config sysname

To set the Cisco wireless LAN controller system name, use the **config sysname** command.

config sysname *name*

Syntax Description

name	System name. The name can contain up to 24 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the system named Ent_01:

```
(Cisco Controller) > config sysname Ent_01
```

Related Commands

show sysinfo

config snmp community accessmode

To modify the access mode (read only or read/write) of an SNMP community, use the **config snmp community accessmode** command.

config snmp community accessmode {**ro** | **rw**} *name*

Syntax Description

ro	Specifies a read-only mode.
rw	Specifies a read/write mode.
name	SNMP community name.

Command Default

Two communities are provided by default with the following settings:

```
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
```

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure read/write access mode for SNMP community:

```
(Cisco Controller) > config snmp community accessmode rw private
```

Related Commands

show snmp community

config snmp community mode

config snmp community create

config snmp community delete

config snmp community ipaddr

config snmp community create

To create a new SNMP community, use the **config snmp community create** command.

config snmp community create *name*

Syntax Description

name	SNMP community name of up to 16 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to create a new community with the default configuration.

The following example shows how to create a new SNMP community named test:

```
(Cisco Controller) > config snmp community create test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community delete

config snmp community ipaddr

config snmp community delete

To delete an SNMP community, use the **config snmp community delete** command.

config snmp community delete *name*

Syntax Description

name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an SNMP community named test:

```
(Cisco Controller) > config snmp community delete test
```

Related Commands

show snmp community

config snmp community mode

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp community ipaddr

To configure the IPv4 or IPv6 address of an SNMP community, use the **config snmp community ipaddr** command.

config snmp community ipaddr *IP addr IPv4 mask/IPv6 Prefix lengthname*

Syntax Description

IP addr	SNMP community IPv4 or IPv6 address.
IPv4 mask/IPv6 Prefix length	SNMP community IP mask (IPv4 mask or IPv6 Prefix length). The IPv6 prefix length is from 0 to 128.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- This command is applicable for both IPv4 and IPv6 addresses.
- This command is not applicable for default SNMP community (public, private).

The following example shows how to configure an SNMP community with the IPv4 address 10.10.10.10, IPv4 mask 255.255.255.0, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 10.10.10.10 255.255.255.0 comaccess
```

The following example shows how to configure an SNMP community with the IPv6 address 2001:9:2:16::1, IPv6 prefix length 64, and SNMP community named comaccess:

```
(Cisco Controller) > config snmp community ipaddr 2001:9:2:16::1 64 comaccess
```

config snmp community mode

To enable or disable an SNMP community, use the **config snmp community mode** command.

config snmp community mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables the community.
disable	Disables the community.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the SNMP community named public:

```
(Cisco Controller) > config snmp community mode disable public
```

Related Commands

show snmp community

config snmp community delete

config snmp community accessmode

config snmp community create

config snmp community ipaddr

config snmp engineID

To configure the SNMP engine ID, use the **config snmp engineID** command.

config snmp engineID {*engine_id* | **default**}

Syntax Description

engine_id	Engine ID in hexadecimal characters (a minimum of 10 and a maximum of 24 characters are allowed).
default	Restores the default engine ID.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The SNMP engine ID is a unique string used to identify the device for administration purposes. You do need to specify an engine ID for the device because a default string is automatically generated using Cisco's enterprise number and the MAC address of the first interface on the device.

If you change the engine ID, then a reboot is required for the change to take effect.

Caution If you change the value of the SNMP engine ID, then the password of the user entered on the command line is converted to an MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm) security digest. This digest is based on both the password and the local engine ID. The command line password is then deleted. Because of this deletion, if the local value of the engine ID changes, the security digests of the SNMP users will become invalid, and the users will have to be reconfigured.

The following example shows how to configure the SNMP engine ID with the value fffffffffff:

```
(Cisco Controller) > config snmp engineID fffffffffff
```

Related Commands

show snmpengineID

config snmp syscontact

To set the SNMP system contact name, use the **config snmp syscontact** command.

config snmp syscontact *contact*

Syntax Description

contact	SNMP system contact name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the SMNP system contact named Cisco WLAN Solution_administrator:

```
(Cisco Controller) > config snmp syscontact Cisco WLAN Solution_administrator
```

config snmp syslocation

To configure the SNMP system location name, use the **config snmp syslocation** command.

config snmp syslocation *location*

Syntax Description

location	SNMP system location name. Valid value can be up to 255 printable characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the SNMP system location name to Building_2a:

```
(Cisco Controller) > config snmp syslocation Building_2a
```

config snmp trapreceiver create

To configure a server to receive SNMP traps, use the **config snmp trapreceiver create** command.

config snmp trapreceiver create *name IP addr*

Syntax Description

name	SNMP community name. The name contain up to 31 characters.
IP addr	Configure the IPv4 or IPv6 address of where to send SNMP traps.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

The IPv4 or IPv6 address must be valid for the command to add the new server.

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 10.1.1.1:

```
(Cisco Controller) > config snmp trapreceiver create test 10.1.1.1
```

The following example shows how to add a new SNMP trap receiver with the SNMP trap receiver named test and IP address 2001:10:1:1::1:

```
(Cisco Controller) > config snmp trapreceiver create test 2001:10:1:1::1
```

config snmp trapreceiver delete

To delete a server from the trap receiver list, use the **config snmp trapreceiver delete** command.

config snmp trapreceiver delete *name*

Syntax Description

name	SNMP community name. The name can contain up to 16 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a server named test from the SNMP trap receiver list:

```
(Cisco Controller) > config snmp trapreceiver delete test
```

Related Commands

show snmp trap

config snmp trapreceiver mode

To send or disable sending traps to a selected server, use the **config snmp trapreceiver mode** command.

config snmp trapreceiver mode {**enable** | **disable**} *name*

Syntax Description

enable	Enables an SNMP trap receiver.
disable	Disables an SNMP trap receiver.
name	SNMP community name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command enables or disables the Cisco wireless LAN controller from sending the traps to the selected server.

The following example shows how to disable an SNMP trap receiver from sending traps to a server named server1:

```
(Cisco Controller) > config snmp trapreceiver mode disable server1
```

Related Commands

show snmp trap

config snmp v3user create

To create a version 3 SNMP user, use the **config snmp v3user create** command.

config snmp v3user create *username* {**ro** | **rw**} {**none** | **hmacmd5** | **hmacsha**} {**none** | **des** | **aescfb128**} [*auth_key*] [*encrypt_key*]

Syntax Description

username	Version 3 SNMP username.
ro	Specifies a read-only user privilege.
rw	Specifies a read-write user privilege.
none	Specifies if no authentication is required.
hmacmd5	Specifies Hashed Message Authentication Coding Message Digest 5 (HMAC-MD5) for authentication.
hmacsha	Specifies Hashed Message Authentication Coding-Secure Hashing Algorithm (HMAC-SHA) for authentication.
none	Specifies if no encryption is required.
des	Specifies to use Cipher Block Chaining-Digital Encryption Standard (CBC-DES) encryption.
aescfb128	Specifies to use Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) encryption.
auth_key	(Optional) Authentication key for the HMAC-MD5 or HMAC-SHA authentication protocol.
encrypt_key	(Optional) Encryption key for the CBC-DES or CFB-AES-128 encryption protocol.

Command Default

SNMP v3 username AccessMode Authentication Encryption

```
-------------------- ------------- -------------- -----------
default              Read/Write    HMAC-SHA       CFB-AES
```

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an SNMP username named test with read-only privileges and no encryption or authentication:

```
(Cisco Controller) > config snmp v3user create test ro none none
```

Related Commands **show snmpv3user**

config snmp v3user delete

To delete a version 3 SNMP user, use the **config snmp v3user delete** command.

config snmp v3user delete *username*

Syntax Description

username	Username to delete.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to remove an SNMP user named test:

```
(Cisco Controller) > config snmp v3user delete test
```

Related Commands

show snmp v3user

config snmp version

To enable or disable selected SNMP versions, use the **config snmp version** command.

config snmp version {**v1** | **v2** | **v3**} {**enable** | **disable**}

Syntax Description

v1	Specifies an SNMP version to enable or disable.
v2	Specifies an SNMP version to enable or disable.
v3	Specifies an SNMP version to enable or disable.
enable	Enables a specified version.
disable	Disables a specified version.

Command Default

By default, all the SNMP versions are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable SNMP version v1:

```
(Cisco Controller) > config snmp version v1 enable
```

Related Commands

show snmpversion

config tacacs acct

To configure TACACS+ accounting server settings, use the **config tacacs acct** command.

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*}

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	Specifies TACACS+ accounting server index from 1 to 3.
IP addr	Specifies IPv4 or IPv6 address of the TACACS+ accounting server.
port	Specifies TACACS+ Server's TCP port.
ascii/hex	Specifies type of TACACS+ server's secret being used (ASCII or HEX).
secret	Specifies secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
server-timeout	Changes the default server timeout for the TACACS+ server.
seconds	Specifies the number of seconds before the TACACS+ server times out. The server timeout range is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv4 address 10.0.0.0, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

The following example shows how to add a new TACACS+ accounting server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs acct add 1  2001:9:6:40::623 10 ascii 12345678
```

The following example shows how to configure the server timeout of 5 seconds for the TACACS+ accounting server:

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

config tacacs auth

To configure TACACS+ authentication server settings, use the **config tacacs auth** command.

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* }

Syntax Description

add	Adds a new TACACS+ accounting server.
1-3	TACACS+ accounting server index from 1 to 3.
IP addr	IP address for the TACACS+ accounting server.
port	Controller port used for the TACACS+ accounting server.
ascii/hex	Type of secret key being used (ASCII or HEX).
secret	Secret key in ASCII or hexadecimal characters.
delete	Deletes a TACACS+ server.
disable	Disables a TACACS+ server.
enable	Enables a TACACS+ server.
mgmt-server-timeout *1-3 seconds*	Changes the default management login server timeout for the server. The number of seconds before server times out is from 1 to 30 seconds.
server-timeout *1-3 seconds*	Changes the default network login server timeout for the server. The number of seconds before server times out is from 5 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv4 address 10.0.0.3, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

The following example shows how to add a new TACACS+ authentication server index 1 with the IPv6 address 2001:9:6:40::623, port number 49, and secret key 12345678 in ASCII:

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

The following example shows how to configure the server timeout for TACACS+ authentication server:

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

config tacacs auth mgmt-server-timeout

To configure a default TACACS+ authentication server timeout for management users, use the **config tacacs auth mgmt-server-timeout** command.

config tacacs auth mgmt-server-timeout *index timeout*

Syntax Description

index	TACACS+ authentication server index.
timeout	Timeout value. The range is 1 to 30 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default TACACS+ authentication server timeout for management users:

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

Related Commands

config tacacs auth

config tacacs dns

To retrieve the TACACS IP information from a DNS server, use the **config radius dns** command.

config radius dns { **global** *port* { *ascii* | *hex* } *secret* | **query** *url timeout* | **serverip** *ip_address* | **disable** | **enable** }

Syntax Description

global	Configures the global port and secret to retrieve the TACACS IP information from a DNS server.
port	Port number for authentication. The range is from 1 to 65535. All the DNS servers should use the same authentication port.
ascii	Format of the shared secret that you should set to ASCII.
hex	Format of the shared secret that you should set to hexadecimal.
secret	TACACS server login secret.
query	Configures the fully qualified domain name (FQDN) of the TACACS server and DNS timeout.
url	FQDN of the TACACS server. The FQDN can be up to 63 case-sensitive, alphanumeric characters.
timeout	Maximum time that the controller waits for, in days, before timing out a request and resending it. The range is from 1 to 180.
serverip	Configures the DNS server IP address.
ip_address	DNS server IP address.
disable	Disables the TACACS DNS feature. The default is disabled.
enable	Enables the controller to retrieve the TACACS IP information from a DNS server.

Command Default

You cannot retrieve the TACACS IP information from a DNS server.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The accounting port is derived from the authentication port. All the DNS servers should use the same secret. When you enable a DNS query, the static configurations will be overridden. The DNS list overrides the static AAA list.

The following example shows how to enable the TACACS DNS feature on the controller:

```
(Cisco Controller) > config tacacs dns enable
```

config tacacs fallback-test interval

To configure TACACS+ probing interval, use the **config tacacs fallback-test interval** command.

config tacacs fallback-test interval { *seconds* }

Syntax Description

seconds	TACACS+ probing interval in seconds. Disable is 0, Range from 180 to 3600 seconds.

Command Default

None

Command History

Release	Modification
8.2	This command was introduced in this release.

The following example shows how to configure TACACS+ probing interval:

```
(Cisco Controller) >  config tacacs fallback-test interval 200
```

config time manual

To set the system time, use the **config time manual** command.

config time manual *MM* | *DD* | *YY HH* : *MM* : *SS*

Syntax Description

MM/*DD*/*YY*	Date.
HH:*MM*:*SS*	Time.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the system date to 04/04/2010 and time to 15:29:00:

```
(Cisco Controller) > config time manual 04/04/2010 15:29:00
```

Related Commands

show time

config time ntp

To set the Network Time Protocol (NTP), use the **config time ntp** command.

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*}

Syntax Description

auth	Configures the NTP authentication.
enable	Enables the NTP authentication.
server-index	NTP server index.
key-index	Key index between 1 and 4294967295.
disable	Disables the NTP authentication.
interval	Configures the NTP version 3 polling interval.
interval	NTP polling interval in seconds. The range is from 3600 and 604800 seconds.
key-auth	Configures the NTP authentication key.
add	Adds an NTP authentication key.
md5	Specifies the authentication protocol.
ascii	Specifies the ASCII key type.
hex	Specifies the hexadecimal key type.
key	Specifies the ASCII key format with a maximum of 16 characters or the hexadecimal key format with a maximum of 32 digits.
delete	Deletes an NTP server.
server	Configures the NTP servers.
IP Address	NTP server's IP address. Use 0.0.0.0 or :: to delete entry.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

- To add the NTP server to the controller, use the **config time ntp server** *index IP Address* command.
- To delete the NTP server (IPv4) from the controller, use the **config time ntp server** *index 0.0.0.0* command.

To delete the NTP server (IPv6) from the controller, use the **config time ntp server** *index ::* command.

- To display configured NTP server on the controller, use the **show time** command.

The following example shows how to configure the NTP polling interval to 7000 seconds:

```
(Cisco Controller) > config time ntp interval 7000
```

The following example shows how to enable NTP authentication where the server index is 4 and the key index is 1:

```
(Cisco Controller) > config time ntp auth enable 4 1
```

The following example shows how to add an NTP authentication key of value ff where the key format is in hexadecimal characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 hex ff
```

The following example shows how to add an NTP authentication key of value ff where the key format is in ASCII characters and the key index is 1:

```
(Cisco Controller) > config time ntp key-auth add 1 md5 ascii ciscokey
```

The following example shows how to add NTP servers and display the servers configured to controllers:

```
(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
```

The following example shows how to delete NTP servers and verify that the servers are deleted removed from the NTP server list:

```
(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

To configure the system time zone, use the **config time timezone** command.

config time timezone {**enable** | **disable**} *delta_hours delta_mins*

Syntax Description

enable	Enables daylight saving time.
disable	Disables daylight saving time.
delta_hours	Local hour difference from the Universal Coordinated Time (UCT).
delta_mins	Local minute difference from UCT.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the daylight saving time:

```
(Cisco Controller) > config time timezone enable 2 0
```

Related Commands

show time

config time timezone location

To set the location of the time zone in order to have daylight saving time set automatically when it occurs, use the **config time timezone location** command.

config time timezone location *location_index*

Syntax Description

location_index	Number representing the time zone required. The time zones are as follows: • (GMT-12:00) International Date Line West • (GMT-11:00) Samoa • (GMT-10:00) Hawaii • (GMT-9:00) Alaska • (GMT-8:00) Pacific Time (US and Canada) • (GMT-7:00) Mountain Time (US and Canada) • (GMT-6:00) Central Time (US and Canada) • (GMT-5:00) Eastern Time (US and Canada) • (GMT-4:00) Atlantic Time (Canada) • (GMT-3:00) Buenos Aires (Argentina) • (GMT-2:00) Mid-Atlantic • (GMT-1:00) Azores • (GMT) London, Lisbon, Dublin, Edinburgh (default value) • (GMT +1:00) Amsterdam, Berlin, Rome, Vienna • (GMT +2:00) Jerusalem • (GMT +3:00) Baghdad • (GMT +4:00) Muscat, Abu Dhabi • (GMT +4:30) Kabul • (GMT +5:00) Karachi, Islamabad, Tashkent • (GMT +5:30) Colombo, Kolkata, Mumbai, New Delhi • (GMT +5:45) Katmandu • (GMT +6:00) Almaty, Novosibirsk • (GMT +6:30) Rangoon • (GMT +7:00) Saigon, Hanoi, Bangkok, Jakatar • (GMT +8:00) Hong Kong, Bejing, Chongquing • (GMT +9:00) Tokyo, Osaka, Sapporo • (GMT +9:30) Darwin • (GMT+10:00) Sydney, Melbourne, Canberra • (GMT+11:00) Magadan, Solomon Is., New Caledonia • (GMT+12:00) Kamchatka, Marshall Is., Fiji • (GMT+12:00) Auckland (New Zealand)

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the location of the time zone in order to set the daylight saving time to location index 10 automatically:

```
(Cisco Controller) > config time timezone location 10
```

Related Commands **show time**

config trapflags 802.11-Security

To enable or disable sending 802.11 security-related traps, use the **config trapflags 802.11-Security** command.

config trapflags 802.11-Security wepDecryptError {**enable** | **disable**}

Syntax Description

enable	Enables sending 802.11 security-related traps.
disable	Disables sending 802.11 security-related traps.

Command Default

By default, sending the 802.11 security-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the 802.11 security related traps:

```
(Cisco Controller) > config trapflags 802.11-Security wepDecryptError disable
```

Related Commands

show trapflags

config trapflags aaa

To enable or disable the sending of AAA server-related traps, use the **config trapflags aaa** command.

config trapflags aaa {**auth** | **servers**} {**enable** | **disable**}

Syntax Description

auth	Enables trap sending when an AAA authentication failure occurs for management user, net user, or MAC filter.
servers	Enables trap sending when no RADIUS servers are responding.
enable	Enables the sending of AAA server-related traps.
disable	Disables the sending of AAA server-related traps.

Command Default

By default, the sending of AAA server-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of AAA server-related traps:

```
(Cisco Controller) > config trapflags aaa auth enable
```

Related Commands

show watchlist

config trapflags adjchannel-rogueap

To configure trap notifications when a rogue access point is detected at the adjacent channel, use the **config trapflags adjchannel-rogueap** command.

config trapflags adjchannel-rogueap {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a rogue access point is detected at the adjacent channel.
disable	Disables trap notifications when a rogue access point is detected at the adjacent channel.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications when a rogue access point is detected at the adjacent channel:

```
(Cisco Controller) > config trapflags adjchannel-rogueap enable
```

Related Commands

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

To enable or disable the sending of Cisco lightweight access point traps, use the **config trapflags ap** command.

config trapflags ap {**register** | **interfaceUp**} {**enable** | **disable**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with Cisco switch.
interfaceUp	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.
enable	Enables sending access point-related traps.
disable	Disables sending access point-related traps.

Command Default

By default, the sending of Cisco lightweight access point traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent traps from sending access point-related traps:

```
(Cisco Controller) > config trapflags ap register disable
```

Related Commands

show trapflags

config trapflags authentication

To enable or disable sending traps with invalid SNMP access, use the **config trapflags authentication** command.

config trapflags authentication {**enable** | **disable**}

Syntax Description

enable	Enables sending traps with invalid SNMP access.
disable	Disables sending traps with invalid SNMP access.

Command Default

By default, the sending traps with invalid SNMP access is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to prevent sending traps on invalid SNMP access:

```
(Cisco Controller) > config trapflags authentication disable
```

Related Commands

show trapflags

config trapflags client

To enable or disable the sending of client-related DOT11 traps, use the **config trapflags client** command.

config trapflags client {**802.11-associate 802.11-disassociate** | **802.11-deauthenticate** | **802.11-authfail** | **802.11-assocfail** | **authentication** | **excluded**} {**enable** | **disable**}

Syntax Description

802.11-associate	Enables the sending of Dot11 association traps to clients.
802.11-disassociate	Enables the sending of Dot11 disassociation traps to clients.
802.11-deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
802.11-authfail	Enables the sending of Dot11 authentication fail traps to clients.
802.11-assocfail	Enables the sending of Dot11 association fail traps to clients.
authentication	Enables the sending of authentication success traps to clients.
excluded	Enables the sending of excluded trap to clients.
enable	Enables sending of client-related DOT11 traps.
disable	Disables sending of client-related DOT11 traps.

Command Default

By default, the sending of client-related DOT11 traps is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of Dot11 disassociation trap to clients:

```
(Cisco Controller) > config trapflags client 802.11-disassociate enable
```

Related Commands

show trapflags

config trapflags client max-warning-threshold

To configure the threshold value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags client max-warning-threshold** command.

config trapflags client max-warning-threshold {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the number of clients that associate with the controller, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The minimum interval between two warnings is 10 mins You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the number of clients that associate with the controller is 90 %.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This table lists the maximum number of clients for different controllers.

Table 9: Maximum Number of Clients Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	7000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	15000
Cisco Flex 7500 Series Controllers	64000
Cisco 8500 Series Controllers	64000
Cisco Virtual Wireless LAN Controllers	30000

The following example shows how to configure the threshold value of the number of clients that associate with the controller:

```
(Cisco Controller) > config trapflags client max-warning-threshold 80
```

Related Commands

show trapflags

config trapflags client

config trapflags configsave

To enable or disable the sending of configuration-saved traps, use the **config trapflags configsave** command.

config trapflags configsave {**enable** | **disable**}

Syntax Description

enable	Enables sending of configuration-saved traps.
disable	Disables the sending of configuration-saved traps.

Command Default

By default, the sending of configuration-saved traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of configuration-saved traps:

```
(Cisco Controller) > config trapflags configsave enable
```

Related Commands

show trapflags

config trapflags IPsec

To enable or disable the sending of IPsec traps, use the **config trapflags IPsec** command.

config trapflags IPsec {**esp-auth** | **esp-reply** | **invalidSPI** | **ike-neg** | **suite-neg** | **invalid-cookie**} {**enable** | **disable**}

Syntax Description

esp-auth	Enables the sending of IPsec traps when an ESP authentication failure occurs.
esp-reply	Enables the sending of IPsec traps when an ESP replay failure occurs.
invalidSPI	Enables the sending of IPsec traps when an ESP invalid SPI is detected.
ike-neg	Enables the sending of IPsec traps when an IKE negotiation failure occurs.
suite-neg	Enables the sending of IPsec traps when a suite negotiation failure occurs.
invalid-cookie	Enables the sending of IPsec traps when a Isakamp invalid cookie is detected.
enable	Enables sending of IPsec traps.
disable	Disables sending of IPsec traps.

Command Default

By default, the sending of IPsec traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of IPsec traps when ESP authentication failure occurs:

```
(Cisco Controller) > config trapflags IPsec esp-auth enable
```

Related Commands

show trapflags

config trapflags linkmode

To enable or disable the controller level link up/down trap flags, use the **config trapflags linkmode** command.

config trapflags linkmode {**enable** | **disable**}

Syntax Description

enable	Enables the controller level link up/down trap flags.
disable	Disables Cisco wireless LAN controller level link up/down trap flags.

Command Default

By default, the controller level link up/down trap flags are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the Cisco wireless LAN controller level link up/down trap:

```
(Cisco Controller) > config trapflags linkmode disable
```

Related Commands

show trapflags

config trapflags mesh

To configure trap notifications when a mesh access point is detected, use the **config trapflags mesh** command.

config trapflags mesh {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications when a mesh access point is detected.
disable	Disables trap notifications when a mesh access point is detected.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications when a mesh access point is detected:

```
(Cisco Controller) > config trapflags mesh enable
```

Related Commands

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

To enable or disable the sending of traps when multiple logins are active, use the **config trapflags multiusers** command.

config trapflags multiusers {**enable** | **disable**}

Syntax Description

enable	Enables the sending of traps when multiple logins are active.
disable	Disables the sending of traps when multiple logins are active.

Command Default

By default, the sending of traps when multiple logins are active is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of traps when multiple logins are active:

```
(Cisco Controller) > config trapflags multiusers disable
```

Related Commands

show trapflags

config trapflags rfid

To configure the threshold value of the maximum number of radio frequency identification (RFID) tags, after which an SNMP trap and a syslog message is sent to the controller, use the **config trapflags rfid** command.

config trapflags rfid {**threshold** | **enable** | **disable**}

Syntax Description

threshold	Configures the threshold percentage value of the maximum number of RFID tags, after which an SNMP trap and a syslog message is sent to the controller. The range is from 80 to 100. The traps and syslog messages are generated every 10 minutes. You cannot configure this interval.
enable	Enables the generation of the traps and syslog messages.
disable	Disables the generation of the traps and syslog messages.

Command Default

The default threshold value of the maximum number of RFID tags is 90 %.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The following table shows the maximum number of RFID tags supported on different controllers:

Table 10: Maximum Number of RFID Tags Supported on Different Controllers

Controller	Maximum Number of Supported Clients
Cisco 5500 Series Controllers	5000
Cisco 2500 Series Controllers	500
Cisco Wireless Services Module 2	10000
Cisco Flex 7500 Series Controllers	50000
Cisco 8500 Series Controllers	50000
Cisco Virtual Wireless LAN Controllers	3000

The following example shows how to configure the threshold value of the maximum number of RFID tags:

```
(Cisco Controller) > config trapflags rfid 80
```

Related Commands

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

To enable or disable sending rogue access point detection traps, use the **config trapflags rogueap** command.

config trapflags rogueap {**enable** | **disable**}

Syntax Description

enable	Enables the sending of rogue access point detection traps.
disable	Disables the sending of rogue access point detection traps.

Command Default

By default, the sending of rogue access point detection traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of rogue access point detection traps:

```
(Cisco Controller) > config trapflags rogueap disable
```

Related Commands

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

To enable or disable the sending of Radio Resource Management (RRM) parameters traps, use the **config trapflags rrm-params** command.

config trapflags rrm-params {**tx-power** | **channel** | **antenna**} {**enable** | **disable**}

Syntax Description

tx-power	Enables trap sending when the RF manager automatically changes the tx-power level for the Cisco lightweight access point interface.
channel	Enables trap sending when the RF manager automatically changes the channel for the Cisco lightweight access point interface.
antenna	Enables trap sending when the RF manager automatically changes the antenna for the Cisco lightweight access point interface.
enable	Enables the sending of RRM parameter-related traps.
disable	Disables the sending of RRM parameter-related traps.

Command Default

By default, the sending of RRM parameters traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the sending of RRM parameter-related traps:

```
(Cisco Controller) > config trapflags rrm-params tx-power enable
```

Related Commands

show trapflags

config trapflags rrm-profile

To enable or disable the sending of Radio Resource Management (RRM) profile-related traps, use the **config trapflags rrm-profile** command.

config trapflags rrm-profile {**load** | **noise** | **interference** | **coverage**} {**enable** | **disable**}

Syntax Description

load	Enables trap sending when the load profile maintained by the RF manager fails.
noise	Enables trap sending when the noise profile maintained by the RF manager fails.
interference	Enables trap sending when the interference profile maintained by the RF manager fails.
coverage	Enables trap sending when the coverage profile maintained by the RF manager fails.
enable	Enables the sending of RRM profile-related traps.
disable	Disables the sending of RRM profile-related traps.

Command Default

By default, the sending of RRM profile-related traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of RRM profile-related traps:

```
(Cisco Controller) > config trapflags rrm-profile load disable
```

Related Commands

show trapflags

config trapflags stpmode

To enable or disable the sending of spanning tree traps, use the **config trapflags stpmode** command.

config trapflags stpmode {**enable** | **disable**}

Syntax Description

enable	Enables the sending of spanning tree traps.
disable	Disables the sending of spanning tree traps.

Command Default

By default, the sending of spanning tree traps is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the sending of spanning tree traps:

```
(Cisco Controller) > config trapflags stpmode disable
```

Related Commands

show trapflags

config trapflags strong-pwdcheck

To configure trap notifications for strong password checks, use the **config trapflags strong-pwdcheck** command.

config trapflags strong-pwdcheck {**enable** | **disable**}

Syntax Description

enable	Enables trap notifications for strong password checks.
disable	Disables trap notifications for strong password checks.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable trap notifications for strong password checks:

```
(Cisco Controller) > config trapflags strong-pwdcheck enable
```

Related Commands

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

To enable or disable Wireless Protection System (WPS) trap sending, use the **config trapflags wps** command.

config trapflags wps {**enable** | **disable**}

Syntax Description

enable	Enables WPS trap sending.
disable	Disables WPS trap sending.

Command Default

By default, the WPS trap sending is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the WPS traps sending:

```
(Cisco Controller) > config trapflags wps disable
```

Related Commands

show trapflags

config tunnel eogre heart-beat

To configure the keep alive ping interval duration, use the **config tunnel eogre** command.

config tunnel eogre heart-beat {**interval** | **max-skip-count**} *number-value*

Syntax Description

interval *number-value*	Time interval between echo request message in seconds.
max-skip-count *number-value*	Maximum number of retries before the member is considered non functional.

Command Default

The default value of heart-beat *interval* is 60 seconds. Range is between 10 to 600 seconds.

The default value of heart-beat *max-skip-count* is 3 retries. Range is between 3 to 10 retries.

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the heart-beat interval value '45 seconds' :

```
config tunnel eogre heart-beat interval 45
```

config tunnel eogre gateway

To configure the Ethernet over GRE gateway IPv4 address, use the **config tunnel eogre gateway** command.

config tunnel eogre gateway { { { **add** | **modify** } *gateway-name* { **ipv4-address** | **ipv6-address** } *gateway-ip-address* } | { **delete** *gateway-name* } }

Syntax Description

add	Adds new gateway.
delete	Removes a gateway.
modify	Modifies an existing gateway.
ipv4-address	To enter the IPv4 address of the gateway.
ipv6-address	To enter the IPv6 address of the gateway.
gateway-ip-address	IPv4 or IPv6 address of the gateway.
gateway-name	Tunnel gateway name.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.
8.3	The IPv6 address format option for the tunnel gateway was added.

- IPv4 address example

```
config tunnel eogre gateway add hurricane ipv4 192.168.10.1
```

- IPv6 address example

```
config tunnel eogre gateway add hurricane ipv6 2001:DB8::1
```

config tunnel eogre domain

To perform tunnel gateway domain configuration, use the **config tunnel eogre domain** command.

config tunnel eogre domain { { **create** | **delete** } *domain-name* } { **add** | **remove** } *domain-name gateway-name*

Syntax Description

create	Creates new gateway domain name.
delete	Deletes gateway domain.
add	Add gateway name to domain
remove	Remove gateway name from domain
domain-name	Domain name
gateway-name	Gateway name

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create new gateway domain name:

```
config tunnel eogre domain create web.com data
```

config tunnel eogre domain primary

To add primary or secondary gateway name to a domain, use the **config tunnel eogre domain primary** command.

config tunnel eogre domain primary *domain-name gateway-name*

Syntax Description

domain-name	Enter the domain name
gateway-name	Enter the gateway name to be added to the domain

Usage Guidelines

In a domain, the primary gateway is active by default. When the primary gateway is not operational, the secondary gateway becomes the active gateway. Clients will have to associate again with the secondary gateway. During and after failover, controller continues to ping the primary gateway. When the primary gateway is operational again, the primary gateway becomes the active gateway. Clients then fall back to the primary gateway. The same option is available for the TGW from FlexConnect in local switched mode. EoGRE tunnels can be DTLS encrypted CAPWAP IPv4 or IPv6. This feature is supported on all Wave 1 and Wave 2 APs that are supported in this release.

Command History

Release	Modification
8.5	This command was introduced.

config tunnel profile

To create, copy, or delete a profile, use the **config tunnel profile** command.

config tunnel profile {**copy** | **create** | **delete**} *profile-name*

Syntax Description

copy	Copies an existing profile.
create	Creates a new profile.
delete	Deletes an existing profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to create a profile:

```
config tunnel profile create floorone
```

config tunnel profile_rule

To add or modify a rule in a profile, use the **config tunnel profile** command.

config tunnel profile rule {**add** | **modify** }*profile-name* **realm-filter** *realm-string* **eogre vlan** *vlan-id gateway-domain-name*

Syntax Description

add	Adds a new rule.
modify	Modifies an existing rule.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to add a rule to a profile:

```
config tunnel profile add table realm filter 5 eogre vlan 3 web.com
```

config tunnel profile_rule-delete

To delete a rule from a profile, use the **config tunnel profile** command.

config tunnel profile ruledelete *profile-name* **realm-filter** *realm-string*

Syntax Description

delete	Deletes an existing rule from a profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to delete a rule from a profile:

```
config tunnel profile delete table realm filter 5
```

config tunnel profile eogre-DHCP82

To enable or disable the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

Syntax Description

enable	Enables DHCP option 82 parameter in the system.
disable	Disables DHCP option 82 parameter in the system.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-gateway-radius-proxy

To enable or disable the gateway-radius-proxy, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **gateway-radius-proxy** {**enable** | **disable**}

Syntax Description

enable	Enables Gateway as Radius Proxy.
disable	Disables Gateway as Radius Proxy.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the gateway proxy:

```
config tunnel profile eogre test gateway-radius-proxy enable
```

config tunnel profile eogre-gateway-radius-proxy-accounting

To enable or disable the gateway as accounting radius-proxy, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **gateway-radius-proxy accounting** {**enable** | **disable**}

Syntax Description

enable	Enables Gateway as accounting Radius Proxy.
disable	Disables Gateway as accounting Radius Proxy.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to disable the gateway as accounting radius proxy:

```
config tunnel profile eogre test gateway-radius-proxy accounting disable
```

config tunnel profile eogre-DHCP82

To enable or disable the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82** {**enable** | **disable**}

Syntax Description

enable	Enables DHCP option 82 parameter in the system.
disable	Disables DHCP option 82 parameter in the system.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-DHCP82-circuit-id

To set format for circuit-id field in DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 circuit-id** *parameter-id*

Syntax Description

circuit-id	Sets the format for the Circuit-ID field in DHCP option 82
parameter-id	List of supported parameters: • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the format for circuit-id in the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 circuit-id access1bldg
```

config tunnel profile eogre-DHCP82-delimiter

To set the delimiter for the DHCP option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 delimiter** *delimiter character*

Syntax Description

delimiter	Sets the delimiter for the DHCP option 82 parameter in the system.
delimiter character	Delimiter is used to separate the DHCP option 82 parameter.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to delimit the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 delimiter -
```

config tunnel profile eogre-DHCP82-format

To set the required format for DCHP option 82, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **dhcp-opt-82 format** {**binary** | **ascii**}

Syntax Description

binary	Set Format for DHCP option 82 as Binary
ascii	Set Format for DHCP option 82 as Ascii

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set 'binary' format to the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 format binary
```

config tunnel profile eogre-DHCP82-remote-id

To set format for remote-id field in DHC P option 82 parameter, use the **config tunnel profile** command.

config tunnel profile eogre *profile-name* **DHCP-Opt-82 remote-id** *parameter-id*

Syntax Description

remote-id	Sets the format for the Remote-ID field in DHCP option 82
parameter-id	List of supported parameters: • ap-mac • ap-ethmac • ap-name • ap-group-name • flex-group-name • ap-location • vlan-id • SSID-name • SSID-TYPE • Client-mac

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to set the format for remote-id in the DHCP option 82 parameter:

```
config tunnel profile eogre test dhcp-opt-82 remote-id access1flr
```

config watchlist add

To add a watchlist entry for a wireless LAN, use the **config watchlist add** command.

config watchlist add {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN.
username *username*	Specifies the name of the user to watch.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

config watchlist delete

To delete a watchlist entry for a wireless LAN, use the **config watchlist delete** command.

config watchlist delete {**mac** *MAC* | **username** *username*}

Syntax Description

mac *MAC*	Specifies the MAC address of the wireless LAN to delete from the list.
username *username*	Specifies the name of the user to delete from the list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete a watchlist entry for the MAC address a5:6b:ac:10:01:6b:

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

config watchlist disable

To disable the client watchlist, use the **config watchlist disable** command.

config watchlist disable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the client watchlist:

```
(Cisco Controller) >config watchlist disable
```

config watchlist enable

To enable a watchlist entry for a wireless LAN, use the **config watchlist enable** command.

config watchlist enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a watchlist entry:

```
(Cisco Controller) >config watchlist enable
```

config wgb vlan

To configure the Workgroup Bridge (WGB) VLAN client support, use the **config wgb vlan** command.

config wgb vlan {**enable** | **disable**}

Syntax Description

enable	Enables wired clients behind a WGB to connect to an anchor controller in a Data Management Zone (DMZ).
disable	Disables wired clients behind a WGB from connecting to an anchor controller in a DMZ.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WGB VLAN client support:

```
(Cisco Controller) >config wgb vlan enable
```

config wlan

To create, delete, enable, or disable a wireless LAN, use the **config wlan** command.

config wlan {**enable** | **disable** | **create** | **delete**} *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

Syntax Description

enable	Enables a wireless LAN.
disable	Disables a wireless LAN.
create	Creates a wireless LAN.
delete	Deletes a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.
name	(Optional) WLAN profile name up to 32 alphanumeric characters.
foreignAp	(Optional) Specifies the third-party access point settings.
ssid	SSID (network name) up to 32 alphanumeric characters.
all	(Optional) Specifies all wireless LANs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you create a new WLAN using the **config wlan create** command, it is created in disabled mode. Leave it disabled until you have finished configuring it.

If you do not specify an SSID, the profile *name* parameter is used for both the profile name and the SSID.

If the management and AP-manager interfaces are mapped to the same port and are members of the same VLAN, you must disable the WLAN before making a port-mapping change to either interface. If the management and AP-manager interfaces are assigned to different VLANs, you do not need to disable the WLAN.

An error message appears if you try to delete a WLAN that is assigned to an access point group. If you proceed, the WLAN is removed from the access point group and from the access point's radio.

The following example shows how to enable wireless LAN identifier 16:

```
(Cisco Controller) >config wlan enable 16
```

config wlan 7920-support

To configure support for phones, use the **config wlan 7920-support** command.

config wlan 7920-support {**client-cac-limit** | **ap-cac-limit**} {**enable** | **disable**} *wlan_id*

Syntax Description

ap-cac-limit	Supports phones that require client-controlled Call Admission Control (CAC) that expect the Cisco vendor-specific information element (IE).
client-cac-limit	Supports phones that require access point-controlled CAC that expect the IEEE 802.11e Draft 6 QBSS-load.
enable	Enables phone support.
disable	Disables phone support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot enable both WMM mode and client-controlled CAC mode on the same WLAN.

The following example shows how to enable the phone support that requires client-controlled CAC with wireless LAN ID 8:

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

config wlan 802.11e

To configure 802.11e support on a wireless LAN, use the **config wlan 802.11e** command.

config wlan 802.11e {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows 802.11e-enabled clients on the wireless LAN.
disable	Disables 802.11e on the wireless LAN.
require	Requires 802.11e-enabled clients on the wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

802.11e provides quality of service (QoS) support for LAN applications, which are critical for delay sensitive applications such as Voice over Wireless IP (VoWIP).

802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay sensitive applications such as voice and video. The 802.11e specification provides seamless interoperability and is especially well suited for use in networks that include a multimedia capability.

The following example shows how to allow 802.11e on the wireless LAN with LAN ID 1:

```
(Cisco Controller) >config wlan 802.11e allow 1
```

config wlan aaa-override

To configure a user policy override via AAA on a wireless LAN, use the **config wlan aaa-override** command.

config wlan aaa-override {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables a policy override.
disable	Disables a policy override.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

AAA is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When AAA override is enabled and a client has conflicting AAA and Cisco wireless LAN controller wireless LAN authentication parameters, client authentication is performed by the AAA server. As part of this authentication, the operating system will move clients from the default Cisco wireless LAN VLAN to a VLAN returned by the AAA server and predefined in the controller interface configuration (only when configured for MAC filtering, 802.1X, and/or WPA operation). In all cases, the operating system will also use QoS, DSCP, 802.1p priority tag values, and ACLs provided by the AAA server, as long as they are predefined in the controller interface configuration. (This VLAN switching by AAA override is also referred to as Identity Networking.)

If the corporate wireless LAN uses a management interface assigned to VLAN 2, and if AAA override returns a redirect to VLAN 100, the operating system redirects all client transmissions to VLAN 100, regardless of the physical port to which VLAN 100 is assigned.

When AAA override is disabled, all client authentication defaults to the controller authentication parameter settings, and authentication is performed by the AAA server if the controller wireless LAN does not contain any client-specific authentication parameters.

The AAA override values might come from a RADIUS server.

The following example shows how to configure user policy override via AAA on WLAN ID 1:

```
(Cisco Controller) >config wlan aaa-override enable 1
```

config wlan acl

To configure a wireless LAN access control list (ACL), use the **config wlan acl** command.

config wlan acl [*acl_name* | **none**]

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
acl_name	(Optional) ACL name.
none	(Optional) Clears the ACL settings for the specified wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a WLAN access control list with WLAN ID 1 and ACL named office_1:

```
(Cisco Controller) >config wlan acl 1 office_1
```

config wlan apgroup

To manage access point group VLAN features, use the **config wlan apgroup** command.

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_name profile_name* | **wlan-radio-policy** *apgroup_name wlan-id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**} | **hotspot** {**venue** {**type** *apgroup_name group_codetype_code* | **name** *apgroup_name language_codevenue_name* } | **operating-class** {**add** | **delete**} *apgroup_name operating_class_value*} }

Syntax Description

add	Creates a new access point group (AP group).
apgroup_name	Access point group name.
wlan_id	Wireless LAN identifier from 1 to 512.
delete	Removes a wireless LAN from an AP group.
description	Describes an AP group.
description	Description of the AP group.
interface-mapping	(Optional) Assigns or removes a Wireless LAN fro
interface_name	(Optional) Interface to which you want to map an A
nac-snmp	Configures NAC SNMP functionality on given AP disables Network Admission Control (NAC) out-o access point group.
enable	Enables NAC out-of-band support on an AP group
disable	Disables NAC out-of-band support on an AP group
NAS-ID	Network Access Server identifier (NAS-ID) for the A is sent to the RADIUS server by the controller (as a the authentication request, which is used to classify u You can enter up to 32 alphanumeric characters. Be and later releases, you can configure the NAS-ID on or an access point group. The order of priority is A WLAN NAS-ID > Interface NAS-ID.
none	Configures the controller system name as the NAS
profile-mapping	Configures RF profile mapping on an AP group.
profile_name	RF profile name for a specified AP group.
wlan-radio-policy	Configures WLAN radio policy on an AP group.

802.11a-only	Configures WLAN radio policy on an AP grou
802.11bg	Configures WLAN radio policy on an AP grou
802.11g-only	Configures WLAN radio policy on an AP grou
all	Configures WLAN radio policy on an AP grou
hotspot	Configures a HotSpot on an AP group.
venue	Configures venue information for an AP group.
type	Configures the type of venue for an AP group.
group_code	Venue group information for an AP group. The following options are available: • 0 : UNSPECIFIED • 1 : ASSEMBLY • 2 : BUSINESS • 3 : EDUCATIONAL • 4 : FACTORY-INDUSTRIAL • 5 : INSTITUTIONAL • 6 : MERCANTILE • 7 : RESIDENTIAL • 8 : STORAGE • 9 : UTILITY-MISC • 10 : VEHICULAR • 11 : OUTDOOR

type_code

Venue type information for an AP group.

For venue group 1 (ASSEMBLY), the followin

- 0 : UNSPECIFIED ASSEMBLY
- 1 : ARENA
- 2 : STADIUM
- 3 : PASSENGER TERMINAL
- 4 : AMPHITHEATER
- 5 : AMUSEMENT PARK
- 6 : PLACE OF WORSHIP
- 7 : CONVENTION CENTER
- 8 : LIBRARY
- 9 : MUSEUM
- 10 : RESTAURANT
- 11 : THEATER
- 12 : BAR
- 13 : COFFEE SHOP
- 14 : ZOO OR AQUARIUM
- 15 : EMERGENCY COORDINATION C

For venue group 2 (BUSINESS), the following

- 0 : UNSPECIFIED BUSINESS
- 1 : DOCTOR OR DENTIST OFFICE
- 2 : BANK
- 3 : FIRE STATION
- 4 : POLICE STATION
- 6 : POST OFFICE
- 7 : PROFESSIONAL OFFICE
- 8 : RESEARCH AND DEVELOPMENT
- 9 : ATTORNEY OFFICE

For venue group 3 (EDUCATIONAL), the follo

- 0 : UNSPECIFIED EDUCATIONAL
- 1 : PRIMARY SCHOOL
- 2 : SECONDARY SCHOOL

- 3 : UNIVERSITY OR COLLEGE

For venue group 4 (FACTORY-INDUSTRIAL), th
available:

- 0 : UNSPECIFIED FACTORY AND INDUS
- 1 : FACTORY

For venue group 5 (INSTITUTIONAL), the followi

- 0 : UNSPECIFIED INSTITUTIONAL
- 1 : HOSPITAL
- 2 : LONG-TERM CARE FACILITY
- 3 : ALCOHOL AND DRUG RE-HABILITAT
- 4 :GROUP HOME
- 5 :PRISON OR JAIL

For venue group 6 (MERCANTILE), the followin

- 0 : UNSPECIFIED MERCANTILE
- 1 : RETAIL STORE
- 2 : GROCERY MARKET
- 3 : AUTOMOTIVE SERVICE STATION
- 4 : SHOPPING MALL
- 5 : GAS STATION

For venue group 7 (RESIDENTIAL), the followin

- 0 : UNSPECIFIED RESIDENTIAL
- 1 : PRIVATE RESIDENCE
- 2 : HOTEL OR MOTEL
- 3 : DORMITORY
- 4 : BOARDING HOUSE

For venue group 8 (STORAGE), the following opt

- 0 : UNSPECIFIED STORAGE

For venue group 9 (UTILITY-MISC), the followi

- 0 : UNSPECIFIED UTILITY AND MISCEL

For venue group 10 (VEHICULAR), the follow

- 0 : UNSPECIFIED VEHICULAR
- 1 : AUTOMOBILE OR TRUCK
- 2 : AIRPLANE
- 3 : BUS
- 4 : FERRY
- 5 : SHIP OR BOAT
- 6 : TRAIN
- 7 : MOTOR BIKE

For venue group 11 (OUTDOOR), the followin

- 0 : UNSPECIFIED OUTDOOR
- 1 : MINI-MESH NETWORK
- 2 : CITY PARK
- 3 : REST AREA
- 4 : TRAFFIC CONTROL
- 5 : BUS STOP
- 6 : KIOSK

name	Configures the name of venue for an AP group.
language_code	An ISO-639 encoded string defining the langua string is a three character language code. For ex for English.
venue_name	Venue name for this AP group. This name is as service set (BSS) and is used in cases where the enough information about the venue. The venue can be up to 252 alphanumeric characters.
add	Adds an operating class for an AP group.
delete	Deletes an operating class for an AP group.
operating_class_value	Operating class for an AP group. The available 83, 84, 112, 113, 115, 116, 117, 118, 119, 120, 126, 127.

Command Default

AP Group VLAN is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

An error message appears if you try to delete an access point group that is used by at least one access point. Before you can delete an AP group in controller software release 6.0, move all APs in this group to another group. The access points are not moved to the default-group access point group as in previous releases. To see the APs, enter the **show wlan apgroups** command. To move APs, enter the **config ap group-name** *groupname cisco_ap* command.

The NAS-ID configured on the controller for AP group or WLAN or interface is used for authentication. The NAS-ID is not propagated across controllers.

The following example shows how to enable the NAC out-of band support on access point group 4:

```
(Cisco Controller) >config wlan apgroup nac enable apgroup 4
```

config wlan apgroup atf 802.11

Configure Cisco Airtime Fairness at an AP group level by using the **config wlan apgroup atf 802.11** command.

config wlan apgroups atf 802.11 {**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-group-name*} | {**optimization** {**enable** | **disable**}}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b/g network settings
mode	Configures the granularity of Cisco ATF enforcement
disable	Disables Cisco ATF
monitor	Configures Cisco ATF in monitor mode
enforce-policy	Configures Cisco ATF in enforcement mode
ap-group-name	AP group name that you must specify
optimization	Configures airtime optimization
enable	Enables airtime optimization
disable	Disabled airtime optimization

Command History

Release	Modification
8.1	This command was introduced

To configure Cisco ATF in enforcement mode on an 802.11a network, for an AP group *my-ap-group*, enter the following command:

```
(Cisco Controller) >config wlan apgroup atf 802.11a mode enforce-policy my-ap-group
```

config wlan apgroup atf 802.11 policy

To configure AP group-level override for Cisco ATF policy on a WLAN by using this command:

config wlan apgroup atf 802.11 {**a** | **b**} **policy** *ap-group-name wlan-id policy-name* **override** {**enable** | **disable**}

Syntax Description

a	Specifies the 802.11a network settings
b	Specifies the 802.11b network settings
policy	Specifies the Cisco ATF policy
ap-group-name	Name of the AP group that you must specify
wlan-id	WLAN ID or Remote LAN ID that you must specify
policy-name	Cisco ATF policy name that you must specify
override	Configures ATF policy override for a WLAN in the AP group
enable	Enables ATF policy override for a WLAN in the AP group
disable	Disables ATF policy override for a WLAN in the AP group

Command History

Release	Modification
8.1	This command was introduced

config wlan apgroup opendns-profile

To configure an open Domain Name System (DNS) profile to an access point (AP) group wireless LAN (WLAN), use the **config wlan apgroup opendns-profile** command.

config wlan apgroup opendns-profile*wlan-id site-name profile-name* **enable**

Syntax Description

wlan-id	WLAN identifier.
site-name	Name of the AP group to configure.
profile-name	OpenDNS profile name used for tracking this profile.
enable	Enables OpenDNS identity.
disable	Disables OpenDNS identity.

Command Default

The OpenDNS profile for an AP group WLAN is not created.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure an openDNS profile to an AP group WLAN:

```
(Cisco Controller) > config wlan apgroup opendns-profile wlan1 site1 user1
```

config wlan apgroup qinq

To configure 802.1Q-in-Q VLAN tagging of traffic for an AP group, use the **config wlan apgroup qinq** command.

config wlan apgroup qinq {**tagging** {**client-traffic | dhcp-v4 | eap-sim-aka**} *apgroup_name* {**enable | disable**} | **service-vlan** *apgroup_name vlan_id*}

Syntax Description

tagging	Configures 802.1Q-in-Q VLAN tagging of traffic.
client-traffic	Configures 802.1Q-in-Q tagging of client traffic for an AP group.
dhcp-v4	Configures 802.1Q-in-Q tagging of DHCPv4 traffic for an AP group.
eap-sim-aka	Configures 802.1Q-in-Q tagging of Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) and EAP for Global System for Mobile Communications Subscriber Identity Module (EAP-SIM) traffic for an AP group.
enable	Enables 802.1Q-in-Q tagging of traffic.
disable	Disables 802.1Q-in-Q tagging of traffic.
service-vlan	Configures service VLAN for an AP group.
apgroup_name	Name of the access point group.
vlan_id	VLAN identifier.

Command Default

By default, 802.1Q-in-Q tagging of client and DHCPv4 traffic for an AP group is disabled.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

Note You must enable 802.1Q-in-Q tagging of client traffic before you enable 802.1Q-in-Q tagging of DHCPv4 traffic.

When you enable 802.1Q-in-Q tagging of client traffic, the 802.1Q-in-Q tagging of EAP-AKA and EAP-SIM traffic is also enabled.

The following example shows how to enable 802.1Q-in-Q tagging of client traffic for an AP group:

```
(Cisco Controller) >config wlan apgroup qinq tagging client-traffic APg1 enable
```

The following example shows how to configure the service VLAN for an AP group:

```
(Cisco Controller) >config wlan apgroup qinq service-vlan APg1 10
```

config wlan assisted-roaming

To configure assisted roaming on a WLAN, use the **config wlan assisted-roaming** command.

config wlan assisted-roaming {**neighbor-list** | **dual-list** | **prediction**} {**enable** | **disable**} *wlan_id*

Syntax Description

neighbor-list	Configures an 802.11k neighbor list for a WLAN.
dual-list	Configures a dual band 802.11k neighbor list for a WLAN. The default is the band that the client is currently associated with.
prediction	Configures an assisted roaming optimization prediction for a WLAN.
enable	Enables the configuration on the WLAN.
disable	Disables the configuration on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

The 802.11k neighbor list is enabled for all WLANs.

By default, dual band list is enabled if the neighbor list feature is enabled for the WLAN.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable the assisted roaming prediction list, a warning appears and load balancing is disabled for the WLAN, if load balancing is already enabled on the WLAN.

The following example shows how to enable an 802.11k neighbor list for a WLAN:

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```

config wlan atf

Map a WLAN to a Cisco ATF policy using the **config wlan atf** command.

config wlan atf *wlan-id* **policy** *policy-id*

Syntax Description

wlan-id	WLAN ID that you must specify to which the Cisco ATF policy has to be mapped.
policy	Specifies the Cisco ATF policy
policy-id	Cisco ATF policy ID that you must specify

Command History

Release	Modification
8.1	This command was introduced

config wlan avc

To configure Application Visibility and Control (AVC) on a WLAN, use the **config wlan avc** command.

config wlan avc *wlan_id* {**profile** *profile_name* | **visibility**} {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
profile	Associates or removes an AVC profile from a WLAN.
profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.
visibility	Configures application visibility on a WLAN.
enable	Enables application visibility on a WLAN. You can view the classification of applications based on the Network Based Application Recognition (NBAR) deep packet inspection technology. Use the **show avc statistics client** command to view the client AVC statistics.
disable	Disables application visibility on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure only one AVC profile per WLAN and each AVC profile can have up to 32 rules. Each rule states a Mark or Drop action for an application, which allows you to configure up to 32 application actions per WLAN. You can configure up to 16 AVC profiles on a controller and associate an AVC profile with multiple WLANs.

The following example shows how to associate an AVC profile with a WLAN:

```
(Cisco Controller) >config wlan avc 5 profile profile1 enable
```

config wlan band-select allow

To configure band selection on a WLAN, use the **config wlan band-select allow** command.

config wlan band-select allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a WLAN.
disable	Disables band selection on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4-GHz and moves the dual band clients to the 5-Ghz spectrum. The band-selection algorithm directs dual-band clients only from the 2.4-GHz radio to the 5-GHz radio of the same access point, and it only runs on an access point when both the 2.4-GHz and 5-GHz radios are up and running. Band selection can be used only with Cisco Aironet 1040, 1140, and 1250 Series and the 3500 series access points.

The following example shows how to enable band selection on a WLAN:

```
(Cisco Controller) >config wlan band-select allow enable 6
```

config wlan broadcast-ssid

To configure an Service Set Identifier (SSID) broadcast on a wireless LAN, use the **config wlan broadcast-ssid** command.

config wlan broadcast-ssid {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Broadcasting of SSID is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an SSID broadcast on wireless LAN ID 1:

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

config wlan call-snoop

To enable or disable Voice-over-IP (VoIP) snooping for a particular WLAN, use the **config wlan call-snoop** command.

config wlan call-snoop {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables VoIP snooping on a wireless LAN.
disable	Disables VoIP snooping on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

WLAN should be with Platinum QoS and it needs to be disabled while invoking this CLI

The following example shows how to enable VoIP snooping for WLAN 3:

```
(Cisco Controller) >config wlan call-snoop 3 enable
```

config wlan chd

To enable or disable Coverage Hole Detection (CHD) for a wireless LAN, use the **config wlan chd** command.

config wlan chd *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables SSID broadcasts on a wireless LAN.
disable	Disables SSID broadcasts on a wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CHD for WLAN 3:

```
(Cisco Controller) >config wlan chd 3 enable
```

config wlan ccx aironet-ie

To enable or disable Aironet information elements (IEs) for a WLAN, use the **config wlan ccx aironet-ie** command.

config wlan ccx aironet-ie {**enable** | **disable**}

Syntax Description

enable	Enables the Aironet information elements.
disable	Disables the Aironet information elements.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable Aironet information elements for a WLAN:

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

config wlan channel-scan defer-priority

To configure the controller to defer priority markings for packets that can defer off channel scanning, use the **config wlan channel-scan defer-priority** command.

config wlan channel-scan defer-priority *priority* [**enable** | **disable**] *wlan_id*

Syntax Description

priority	User priority value (0 to 7).
enable	(Optional) Enables packet at given priority to defer off channel scanning.
disable	(Optional) Disables packet at gven priority to defer off channel scanning.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The priority value should be set to 6 on the client and on the WLAN.

The following example shows how to enable the controller to defer priority markings that can defer off channel scanning with user priority value 6 and WLAN id 30:

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```

config wlan channel-scan defer-time

To assign the channel scan defer time in milliseconds, use the **config wlan channel-scan defer-time** command.

config wlan channel-scan defer-time *msecs wlan_id*

Syntax Description

msecs	Deferral time in milliseconds (0 to 60000 milliseconds).
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on your WLAN.

The following example shows how to assign the scan defer time to 40 milliseconds for WLAN with ID 50:

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

config wlan custom-web

To configure the web authentication page for a WLAN, use the **config wlan custom-web** command.

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* } }

Syntax Description

ext-webauth-url	Configures an external web authentication URL.
ext-webauth-url	External web authentication URL.
wlan_id	WLAN identifier. Default range is from 1 to 512.
global	Configures the global status for a WLAN.
enable	Enables the global status for a WLAN.
disable	Disables the global status for a WLAN.
ms-open	Configures the ms-open feature on the WLAN.
enable	Enables the ms-open feature on the WLAN.
disable	Disables the ms-open feature on the WLAN.
url	Configures ms-open URL.
login-page	Configures the name of the login page for an external web authentication URL.
page-name	Login page name for an external web authentication URL.
loginfailure-page	Configures the name of the login failure page for an external web authentication URL.
none	Does not configure a login failure page for an external web authentication URL.
logout-page	Configures the name of the logout page for an external web authentication URL.
sleep-client	Configures the sleep client feature on the WLAN.
timeout	Configures the sleep client timeout on the WLAN.
duration	Maximum amount of time after the idle timeout, in hours, before a sleeping client is forced to reauthenticate. The range is from 1 to 720. The default is 12. When the sleep client feature is enabled, the clients need not provide the login credentials when they move from one controller to another (if the controllers are in the same mobility group) between the sleep and wake-up times.
webauth-type	Configures the type of web authentication for the WLAN.
internal	Displays the default login page.

customized	Displays a customized login page.
external	Displays a login page on an external web server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2	This command was modified and the ms-open parameters were added.

The following example shows how to configure web authentication type in the WLAN.

```
Cisco Controller config wlan custom-web webauth-type external
```

config wlan dhcp_server

To configure the internal DHCP server for a wireless LAN, use the **config wlan dhcp_server** command.

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	IP address of the internal DHCP server (this parameter is required).
required	(Optional) Specifies whether DHCP address assignment is required.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The preferred method for configuring DHCP is to use the primary DHCP address assigned to a particular interface instead of the DHCP server override. If you enable the override, you can use the **show wlan** command to verify that the DHCP server has been assigned to the WLAN.

The following example shows how to configure an IP address 10.10.2.1 of the internal DHCP server for wireless LAN ID 16:

```
(Cisco Controller) >config wlan dhcp_server 16 10.10.2.1
```

config wlan diag-channel

To enable the diagnostic channel troubleshooting on a particular WLAN, use the **config wlan diag-channel** command.

config wlan diag-channel [**enable** | **disable**] *wlan_id*

Syntax Description

enable	(Optional) Enables the wireless LAN diagnostic channel.
disable	(Optional) Disables the wireless LAN diagnostic channel.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the wireless LAN diagnostic channel for WLAN ID 1:

```
(Cisco Controller) >config wlan diag-channel enable 1
```

config wlan dtim

To configure a Delivery Traffic Indicator Message (DTIM) for 802.11 radio network **config wlan dtim** command.

config wlan dtim {**802.11a** | **802.11b**} *dtim wlan_id*

Syntax Description

802.11a	Configures DTIM for the 802.11a radio network.
802.11b	Configures DTIM for the 802.11b radio network.
dtim	Value for DTIM (between 1 to 255 inclusive).
wlan_id	Number of the WLAN to be configured.

Command Default

The default is DTIM 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure DTIM for 802.11a radio network with DTIM value 128 and WLAN ID 1:

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

config wlan exclusionlist

To configure the wireless LAN exclusion list, use the **config wlan exclusionlist** command.

config wlan exclusionlist {*wlan_id* [**enabled** | **disabled** | *time*] | **foreignAp** [**enabled** | **disabled** | *time*]}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enabled	(Optional) Enables the exclusion list for the specified wireless LAN or foreign access point.
disabled	(Optional) Disables the exclusion list for the specified wireless LAN or a foreign access point.
time	(Optional) Exclusion list timeout in seconds. A value of zero (0) specifies infinite time.
foreignAp	Specifies a third-party access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command replaces the **config wlan blacklist** command.

The following example shows how to enable the exclusion list for WLAN ID 1:

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

config wlan fabric

To enable or disable fabric on a WLAN, use the **config wlan fabric** command.

config wlan fabric { **enable** | **disable** } *wlan-id*

Syntax Description

enable	Enables fabric on a WLAN.
disable	Disables fabric on a WLAN.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

Non-fabric APs are not configured with fabric WLAN.

Example

The following example shows how to enable fabric on a WLAN:

```
config wlan fabric enable wlan1
```

config wlan fabric acl

To configure access control list (ACL) name for the fabric WLAN, use the **config wlan fabric acl** command.

config wlan fabric acl *flex-acl-name wlan-id*

Syntax Description

flex-acl-name	ACL name.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

The ACL to be used comes from the Flex ACL table.

Examples

The following example shows how to configure an ACL name for the fabric WLAN:

```
(Cisco Controller) >config wlan fabric acl flexACL wlan1
```

config wlan fabric avc-policy

To configure an Application Visibility and Control (AVC) profile name for the fabric WLAN, use the **config wlan fabric avc-policy** command.

config wlan fabric avc-policy *flex-avc-policy-name* *wlan-id*

Syntax Description

flex-avc-policy-name	AVC policy name.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Examples

The following example shows how to configure an AVC profile name for the fabric WLAN:

```
(Cisco Controller) >config wlan fabric acl AVCpolicy wlan1
```

config wlan fabric encap vxlan

To map a Virtual Extensible LAN (VXLAN) network identifier (VNID) to a WLAN, use the **config wlan fabric encap vxlan** command.

config wlan fabric encap vxlan*wlan-id*

Syntax Description

wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Examples

The following example shows how to map a VNID to a WLAN:

```
(Cisco Controller) >config wlan fabric encap vxlan wlan1
```

config wlan fabric switch-ip

To configure the IP address of the Fabric Switch that is used for the AP VXLAN tunnel, use the **config wlan fabric switch-ip** command.

config wlan fabric switch-ip *ip-address wlan-id*

Syntax Description

ip-address	IP address of the switch.
wlan-id	WLAN identifier.

Command Default

Command Modes

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

This command is optional for the fabric configuration, and is mainly used for guest AP tunnel. If fabric is enabled, the Switch IP where AP is connected is searched by default. You can set IP as 0.0.0.0 to disable the configuration and revert to the default configuration.

Examples

The following example shows how to configure the IP address of the Fabric Switch that is used for the AP VXLAN tunnel:

```
(Cisco Controller) >config wlan fabric switch-ip 209.165.200.224 wlan1
```

config wlan fabric tag

To configure security group tag (SGT) on a WLAN, use the **config wlan fabric tag** command.

config wlan fabric tag *sgt* *wlan-id*

Syntax Description

sgt	Security group tag.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

To disable SGT on a WLAN, use zero at the *sgt* variable.

Ideally SGT should be acquired during authentication from the RADIUS server. For guests, this value can be configured. The default value is 0.

Examples

The following example shows how to configure SGT on a WLAN:

```
(Cisco Controller) >config wlan fabric tag sgt1 wlan1
```

The following example shows how to disable SGT from a WLAN:

```
(Cisco Controller) >config wlan fabric tag 0 wlan1
```

config wlan fabric vnid

To configure Virtual Extensible LAN (VXLAN) network identifier (VNID) on a fabric WLAN, use the **config wlan fabric vnid** command.

config wlan fabric vnid *vnid wlan-id*

Syntax Description

vnid	VXLAN network identifier.
wlan-id	WLAN identifier.

Command Default

None

Command History

Release	Modification
8.5	This command was introduced.

Usage Guidelines

To remove VXLAN mapping from a WLAN, use zero at the *vnid* variable.

The interface or VLAN mapping on the WLAN will be done on the switch.

Examples

The following example shows how to config VNID on a fabric WLAN:

```
(Cisco Controller) >config wlan fabric vnid1 wlan1
```

The following example shows how to remove VNID mapping from a fabric WLAN:

```
(Cisco Controller) >config wlan fabric 0 wlan1
```

config wlan flexconnect ap-auth

To configure local authentication of clients associated with FlexConnect on a locally switched WLAN, use the **config wlan flexconnect ap-auth** command.

config wlan flexconnect ap-auth *wlan_id* {**enable** | **disable**}

Syntax Description

ap-auth	Configures local authentication of clients associated with an FlexConnect on a locally switched WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables AP authentication on a WLAN.
disable	Disables AP authentication on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Local switching must be enabled on the WLAN where you want to configure local authentication of clients associated with FlexConnect.

The following example shows how to enable authentication of clients associated with FlexConnect on a specified WLAN:

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```

config wlan flexconnect central-assoc

To configure client reassociation and security key caching on the controller, use the **config wlan flexconnect central-assoc** command.

config wlan flexconnect central-assoc *wlan-id* { **enable** | **disable** }

Syntax Description

wlan-id	ID of the WLAN
enable	Enables client reassociation and security key caching on the controller
disable	Disables client reassociation and security key caching on the controller

Command Default

Client reassociation and security key caching on the controller is in the disabled state.

Command History

Release	Modification
8.0	This command was introduced.

Usage Guidelines

A use case for this configuration is a large-scale deployment with fast roaming.

Configuration of central association with local authentication is not supported for the WLAN. After the PMIPv6 tunnel is set up, all data traffic from the PMIPv6 clients are forwarded from the Cisco AP to the local mobility anchor (LMA) in the Generic Routing Encapsulation (GRE) tunnel. If the connectivity between the Cisco AP and the controller is lost, the data traffic for the existing PMIPv6 clients continues to flow until the connectivity between the Cisco AP and the client is lost. When the AP is in stand-alone mode, no new client associations are accepted on the PMIPv6-enabled WLAN.

The following example shows how to enable client reassociation and security key caching on the controller for a WLAN whose ID is 2:

```
(Cisco Controller) >config wlan flexconnect central-assoc 2 enable
```

config wlan flexconnect learn-ipaddr

To enable or disable client IP address learning for the Cisco WLAN controller, use the **config wlan flexconnect learn-ipaddr** command.

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables client IPv4 address learning on a wireless LAN.
disable	Disables client IPv4 address learning on a wireless LAN.

Command Default

Disabled when the **config wlan flexconnect local-switching** command is disabled. Enabled when the **config wlan flexconnect local-switching** command is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address, and the controller will periodically drop the client. Disable this option to keep the client connection without waiting to learn the client IP address.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to disable client IP address learning for WLAN 6:

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

Related Commands

show wlan

config wlan flexconnect local-switching

To configure local switching, central DHCP, NAT-PAT, or the override DNS option on a FlexConnect WLAN, use the **config wlan flexconnect local switching** command.

config wlan flexconnect local-switching *wlan_id* {**enable** | **disable**} { {**central-dhcp** {**enable** | **disable**} **nat-pat** {**enable** | **disable**} } | {**override option dns** { **enable** | **disable**} } }

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables local switching on a FlexConnect WLAN.
disable	Disables local switching on a FlexConnect WLAN.
central-dhcp	Configures central switching of DHCP packets on the local s When you enable this feature, the DHCP packets received fr to the controller and forwarded to the corresponding VLAN
enable	Enables central DHCP on a FlexConnect WLAN.
disable	Disables central DHCP on a FlexConnect WLAN.
nat-pat	Configures Network Address Translation (NAT) and Port Ad local switching FlexConnect WLAN.
enable	Enables NAT-PAT on the FlexConnect WLAN.
disable	Disables NAT-PAT on the FlexConnect WLAN.
override	Specifies the DHCP override options on the FlexConnect W
option dns	Specifies the override DNS option on the FlexConnect WLA the clients get their DNS server IP address from the AP, not f
enable	Enables the override DNS option on the FlexConnect WLAN
disable	Disables the override DNS option on the FlexConnect WLA

Command Default

This feature is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

When you enable the **config wlan flexconnect local-switching** command, the **config wlan flexconnect learn-ipaddr** command is enabled by default.

Note This command is valid only for IPv4.

Note The ability to disable IP address learning is not supported with FlexConnect central switching.

The following example shows how to enable WLAN 6 for local switching and enable central DHCP and NAT-PAT:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable
nat-pat enable
```

The following example shows how to enable the override DNS option on WLAN 6:

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect vlan-central-switching

To configure central switching on a locally switched WLAN, use the **config wlan flexconnect vlan-central-switching** command.

config wlan flexconnect vlan-central-switching *wlan_id* { **enable** | **disable** }

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables central switching on a locally switched wireless LAN.
disable	Disables central switching on a locally switched wireless LAN.

Command Default

Central switching is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must enable Flexconnect local switching to enable VLAN central switching. When you enable WLAN central switching, the access point bridges the traffic locally if the WLAN is configured on the local IEEE 802.1Q link. If the VLAN is not configured on the access point, the AP tunnels the traffic back to the controller and the controller bridges the traffic to the corresponding VLAN.

WLAN central switching does not support:

- FlexConnect local authentication.
- Layer 3 roaming of local switching client.

The following example shows how to enable WLAN 6 for central switching:

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```

config wlan flow

To associate a NetFlow monitor with a WLAN, use the **config wlan flow** command.

config wlan flow *wlan_id* **monitor** *monitor_name* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512 (inclusive).
monitor	Configures a NetFlow monitor.
monitor_name	Name of the NetFlow monitor. The monitor name can be up to 32 case-sensitive, alphanumeric characters. You cannot include spaces for a monitor name.
enable	Associates a NetFlow monitor with a WLAN.
disable	Dissociates a NetFlow monitor from a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use the **config flow** command to create a new NetFlow monitor.

The following example shows how to associate a NetFlow monitor with a WLAN:

```
(Cisco Controller) >config wlan flow 5 monitor monitor1 enable
```

config wlan hotspot

To configure a HotSpot on a WLAN, use the **config wlan hotspot** command.

config wlan hotspot {**clear-all** *wlan_id* | **dot11u** | **hs2** | **msap**}

Syntax Description

clear-all	Clears the HotSpot configurations on a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
dot11u	Configures an 802.11u HotSpot on a WLAN.
hs2	Configures HotSpot2 on a WLAN.
msap	Configures the Mobility Services Advertisement Protocol (MSAP) on a WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can configure up to 32 HotSpot WLANs.

The following example shows how to configure HotSpot2 for a WLAN:

```
(Cisco Controller) >config wlan hotspot hs2 enable 2
```

config wlan hotspot dot11u

To configure an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u** command.

config wlan hotspot dot11u {**3gpp-info** | **auth-type** | **enable** | **disable** | **domain** | **hessid** | **ipaddr-type** | **nai-realm** | **network-type** | **roam-oi**}

Syntax Description

3gpp-info	Configures 3GPP cellular network information.
auth-type	Configures the network authentication type.
disable	Disables 802.11u on the HotSpot profile.
domain	Configures a domain.
enable	Enables 802.11u on the HotSpot profile. IEEE 802.11u enables automatic WLAN offload for 802.1X devices at the HotSpot of mobile or roaming partners.
hessid	Configures the Homogenous Extended Service Set Identifier (HESSID). The HESSID is a 6-octet MAC address that uniquely identifies the network.
ipaddr-type	Configures the IPv4 address availability type.
nai-realm	Configures a realm for 802.11u enabled WLANs.
network-type	Configures the 802.11u network type and Internet access.
roam-oi	Configures the roaming consortium Organizational Identifier (OI) list.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to enable 802.11u on a HotSpot profile:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u 3gpp-info

To configure 3GPP cellular network information on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u 3gpp-info** command.

config wlan hotspot dot11u 3gpp-info {**add** | **delete**} *index country_code network_code wlan_id*

Syntax Description

add	Adds mobile cellular network information.
delete	Deletes mobile cellular network information.
index	Cellular index. The range is from 1 to 32.
country_code	Mobile Country Code (MCC) in Binary Coded Decimal (BCD) format. The country code can be up to 3 characters. For example, the MCC for USA is 310.
network_code	Mobile Network Code (MNC) in BCD format. An MNC is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile phone operator or carrier. The network code can be up to 3 characters. For example, the MNC for T- Mobile is 026.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Number of mobile network codes supported is 32 per WLAN.

The following example shows how to configure 3GPP cellular network information on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add
```

config wlan hotspot dot11u auth-type

To configure the network authentication type on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u auth-type** command.

config wlan hotspot dot11u auth-type *network-auth wlan_id*

Syntax Description

network-auth	Network authentication that you would like to configure on the WLAN. The available values are as follows: • 0—Acceptance of terms and conditions • 1—On-line enrollment • 2—HTTP/HTTPS redirection • 3—DNS Redirection • 4—Not Applicable
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The DNS redirection option is not supported in Release 7.3.

The following example shows how to configure HTTP/HTTPS redirection as the network authentication type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u auth-type 2 1
```

config wlan hotspot dot11u disable

To disable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u disable** command.

config wlan hotspot dot11u disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u disable 6
```

config wlan hotspot dot11u domain

To configure a domain operating in the 802.11 access network, use the **config wlan hotspot dot11u domain** command.

config wlan hotspot dot11u domain {**add** *wlan_id domain-index domain_name* | **delete** *wlan_id domain-index* | **modify** *wlan_id domain-index domain_name*}

Syntax Description

add	Adds a domain.
wlan_id	Wireless LAN identifier between 1 and 512.
domain-index	Domain index in the range 1 to 32.
domain_name	Domain name. The domain name is case sensitive and can be up to 255 alphanumeric characters.
delete	Deletes a domain.
modify	Modifies a domain.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a domain in the 802.11 access network:

```
(Cisco Controller) >config wlan hotspot dot11u domain add 6 30 domain1
```

config wlan hotspot dot11u enable

To enable an 802.11u HotSpot on a WLAN, use the **config wlan hotspot dot11u enable** command.

config wlan hotspot dot11u enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable an 802.11u HotSpot on a WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u hessid

To configure a Homogenous Extended Service Set Identifier (HESSID) on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u hessid** command.

config wlan hotspot dot11u hessid *hessid wlan_id*

Syntax Description

hessid	MAC address that can be configured as an HESSID. The HESSID is a 6-octet MAC address that uniquely identifies the network. For example, Basic Service Set Identification (BSSID) of the WLAN can be used as the HESSID.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an HESSID on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```

config wlan hotspot dot11u ipaddr-type

To configure the type of IP address available on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u ipaddr-type** command.

config wlan hotspot dot11u ipaddr-type *IPv4Type* {*0 - 7*} *IPv6Type* {*0 - 2*}*wlan_id*

Syntax Description

IPv4Type	IPv4 type address. Enter one of the following values: 0—IPv4 address not available. 1—Public IPv4 address available. 2—Port restricted IPv4 address available. 3—Single NAT enabled private IPv4 address available. 4—Double NAT enabled private IPv4 address available. 5—Port restricted IPv4 address and single NAT enabled IPv4 address available. 6—Port restricted IPv4 address and double NAT enabled IPv4 address available. 7— Availability of the IPv4 address is not known.
IPv6Type	IPv6 type address. Enter one of the following values: 0—IPv6 address not available. 1—IPv6 address available. 2—Availability of the IPv6 address is not known.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default values for IPv4 type address is 1.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to configure the IP address availability type on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u ipaddr-type 6 2 6
```

Related Commands

show wlan

config wlan hotspot dot11u nai-realm

To configure realms for an 802.11u HotSpot WLANs, use the **config wlan hotspot dot11u nai-realm** command.

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*}

Syntax Description

add	Adds a realm.
delete	Deletes a realm.
modify	Modifies a realm.
auth-method	Specifies the authentication method used.
wlan_id	Wireless LAN identifier from 1 to 512.
realm-index	Realm index. The range is from 1 to 32.
eap-index	EAP index. The range is from 1 to 4.
auth-index	Authentication index value. The range is from 1 to 10.
auth-method	Authentication method to be used. The range is from 1 to 4. The following options are available: • 1—Non-EAP Inner Auth Method • 2—Inner Auth Type • 3—Credential Type • 4—Tunneled EAP Method Credential Type
auth-parameter	Authentication parameter to use. This value depends on the authentication method used. See the following table for more details.
eap-method	Specifies the Extensible Authentication Protocol (EAP) method used.

eap-method	EAP Method. The range is from 0 to 7. The following options are available: • 0—Not Applicable • 1—Lightweight Extensible Authentication Protocol (LEAP) • 2—Protected EAP (PEAP) • 3—EAP-Transport Layer Security (EAP-TLS) • 4—EAP-FAST (Flexible Authentication via Secure Tunneling) • 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	Specifies the name of the realm.
realm	Name of the realm. The realm name should be RFC 4282 compliant. For example, Cisco. The realm name is case-sensitive and can be up to 255 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This table lists the authentication parameters.

Table 11: Authentication Parameters

Non-EAP Inner Method(1)	Inner Authentication EAP Method Type(2)	Credential Type(3)/Tunneled EAP Credential Type(4)
0—Reserved 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 Secure Element 4—Hardware Token 5—Soft Token 6—Certificate 7—Username/Password 8—Reserver 9—Anonymous 10—Vendor Specific

The following example shows how to add the Tunneled EAP Method Credential authentication method on WLAN 4:

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

config wlan hotspot dot11u network-type

To configure the network type and internet availability on an 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u network-type** command.

config wlan hotspot dot11u network-type *wlan_id network-type internet-access*

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
network-type	Network type. The available options are as follows: • 0—Private Network • 1—Private Network with Guest Access • 2—Chargeable Public Network • 3—Free Public Network • 4—Personal Device Network • 5—Emergency Services Only Network • 14—Test or Experimental • 15—Wildcard
internet-access	Internet availability status. A value of zero indicates no Internet availability and 1 indicates Internet availability.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the network type and Internet availability on an 802.11u HotSpot WLAN:

```
(Cisco Controller) >config wlan hotspot dot11u network-type 2 1
```

config wlan hotspot dot11u roam-oi

To configure a roaming consortium Organizational Identifier (OI) list on a 802.11u HotSpot WLAN, use the **config wlan hotspot dot11u roam-oi** command.

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*}

Syntax Description

add	Adds an OI.
wlan-id	Wireless LAN identifier from 1 to 512.
oi-index	Index in the range 1 to 32.
oi	Number that must be a valid 6 digit hexadecimal number and 6 bytes in length. For example, 004096 or AABBDF.
is-beacon	Beacon flag used to add an OI to the beacon. 0 indicates disable and 1 indicates enable. You can add a maximum of 3 OIs for a WLAN with this flag set.
modify	Modifies an OI.
delete	Deletes an OI.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the roaming consortium OI list:

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

config wlan hotspot hs2

To configure the HotSpot2 parameters, use the **config wlan hotspot hs2** command.

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* }

Syntax Description

disable	Disables HotSpot2.
wlan-id	Wireless LAN identifier from 1 to 512.
enable	Enables HotSpot2.
operator-name	Specifies the name of the 802.11 operator.
add	Adds the operator name, port configuration, or WAN metrics parameters to the WLAN configuration.
index	Index of the operator. The range is from 1 to 32.
operator-name	Name of the operator.
language-code	Language used. An ISO-14962-1997 encoded string that defin language. This string is a three character language code. Ente first three letters of the language in English. For example, eng English.
delete	Deletes the operator name, port configuration, or WAN metri parameters from the WLAN.
modify	Modifies the operator name, port configuration, or WAN met parameters of the WLAN.
port-config	Configures the port configuration values.
port_config_index	Port configuration index. The range is from 1 to 32. The defa value is 1.
ip-protocol	Protocol to use. This parameter provides information on the connection status of the most commonly used communication protocols and ports. The following options are available: 1—ICMP 6—FTP/SSH/TLS/PPTP-VPN/VoIP 17—IKEv2 (IPSec-VPN/VoIP/ESP) 50—ESP (IPSec-VPN)

port-number	Port number. The following options are available: 0—ICMP/ESP (IPSec-VPN) 20—FTP 22—SSH 443—TLS-VPN 500—IKEv2 1723—PPTP-VPN 4500—IKEv2 5060—VoIP
status	Status of the IP port. The following options are available: 0—Closed 1—Open 2—Unknown
wan-metrics	Configures the WAN metrics.
link-status	Link status. The following options are available: • 0—Unknown • 1—Link up • 2—Link down • 3—Link in test state
symet-link	Symmetric link status. The following options are available: • 0—Link speed is different for uplink and downlink. For example: ADSL • 1—Link speed is the same for uplink and downlink. For example: DS1
downlink-speed	Downlink speed of the WAN backhaul link in kbps. Maximum valu is 4,194,304 kbps.
uplink-speed	Uplink speed of the WAN backhaul link in kbps. The maximum value is 4,194,304 kbps.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WAN metrics parameters:

```
(Cisco Controller) >config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

config wlan hotspot hs2 domain-id

To configure a domain ID, use the **config wlan hotspot hs2 domain-id** command in WLAN configuration mode.

config wlan hotspot hs2 domain-id *wlan-id domain-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
domain-id	Domain ID. Enter a value between 0 to 65535.

Command Default

The domain ID is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure a domain ID:

```
Cisco Controller > config wlan hotspot hs2 domain-id 12 2
```

config wlan hotspot hs2 osu legacy-ssid

To configure Online Sign Up (OSU) Service Set Identifier (SSID) name, use the **config wlan hotspot hs2 osu legacy-ssid** command in WLAN configuration mode.

config wlan hotspot hs2 osu legacy-ssid *wlan-id ssid-name*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
ssid-name	SSID name.

Command Default

OSU SSID name is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU SSID name:

```
Cisco Controller > config wlan hotspot hs2 osu legacy-ssid 12 cisco
```

config wlan hotspot hs2 osu sp create

To create the Online Sign Up (OSU) service provider name, use the **config wlan hotspot hs2 osu sp create** command in WLAN configuration node.

config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code* **ascii/hex** *friendly-name* [*description*]

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
lang-code	Language code. Enter 2 or 3 letters from ISO-639, for example,*eng* for English.
ascii/hex	Specifies the text format, whether ASCII or Hex.
friendly-name	Service provider name. The maximum limit is 252 characters.
description	(Optional) Server description. The maximum limit is 252 characters.

Command Default

The OSU service provider name is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU service provider name:

```
Cisco Controller > config wlan hotspot hs2 osu sp create 12 2 eng ascii cisco server-1
```

config wlan hotspot hs2 osu sp delete

To delete the Online Sign Up (OSU) service provider, use the **config wlan hotspot hs2 osu sp delete** command.

config wlan hotspot hs2 osu sp delete *wlan-idosu-index lang-code*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
lang-code	Language code. Enter 2 or 3 letters from ISO-639, for example, *eng* for English.

Command Default

The OSU service provider is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU service provider:

```
Cisco Controller > config wlan hotspot hs2 osu sp delete 12 2 eng
```

config wlan hotspot hs2 osu sp icon-file add

To configure an Online Sign Up (OSU) icon file on a particular WLAN, use the **config wlan hotspot hs2 osu sp icon-file add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp icon-file add *wlan-idosu-index icon-filename*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
icon-filename	Filename of the icon.

Command Default

The OSU icon file is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

Usage Guidelines

Before using this command, configure icon parameters using the **config icon** *file-info* command.

This example shows how to configure an OSU icon file on a WLAN:

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file add 12 2 test-icon
```

config wlan hotspot hs2 osu sp icon-file delete

To delete an Online Sign Up (OSU) icon file from a WLAN, use the **config wlan hotspot hs2 osu sp icon-file delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp icon-file delete *wlan-idosu-index icon-filename*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
icon-filename	Filename of the icon.

Command Default

The OSU icon file is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU icon file from a WLAN:

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file delete 12 2 test-icon
```

config wlan hotspot hs2 osu sp method add

To configure an Online Sign Up (OSU) method list, use the **config wlan hotspot hs2 osu sp method add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-primary method-secondary*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
method-primary	Primary OSU encoding method. Valid values are: **oma-dm** or **soap-xml**.
method-secondary	(Optional) Secondary OSU encoding method. Valid values are: **oma-dm** or **soap-xml**.

Command Default

The OSU method list is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU method list:

```
Cisco Controller > config wlan hotspot hs2 osu sp method add 12 2 oma-dm oma-dm
```

config wlan hotspot hs2 osu sp method delete

To delete an Online Sign Up (OSU) method list, use the **config wlan hotspot hs2 osu sp method delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
method	The OSU encoding method. Valid values are **oma-dm** or **soap-xml**.

Command Default

The OSU method list is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU method list:

```
Cisco Controller > config wlan hotspot hs2 osu sp method delete 12 2 oma-dm
```

config wlan hotspot hs2 osu sp nai add

To create an Online Sign Up (OSU) Network Access Identifier (NAI), use the **config wlan hotspot hs2 osu sp nai add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
nai	OSU Server NAI. Enter a name within a maximum limit of 255 characters.

Command Default

The OSU NAI is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure an OSU NAI:

```
Cisco Controller > config wlan hotspot hs2 osu sp nai add 12 2 nai-1
```

config wlan hotspot hs2 osu sp nai delete

To delete an Online Sign Up (OSU) Network Access Identifier (NAI), use the **config wlan hotspot hs2 osu sp nai delete** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.

Command Default

The OSU NAI is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU NAI:

```
Cisco Controller > config wlan hotspot hs2 osu sp nai delete 12 2
```

config wlan hotspot hs2 osu sp uri add

To create an Online Sign Up (OSU) URI, use the **config wlan hotspot hs2 osu sp uri add** command in WLAN configuration mode.

config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.
uri	OSU server name. Enter a Uniform Resource Identifier (URI) with a maximum of 255 characters.

Command Default

The OSU URI is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to create an OSU URI:

```
Cisco Controller > config wlan hotspot hs2 osu sp uri add 12 2 server
```

config wlan hotspot hs2 osu sp uri delete

To delete an Online Sign Up (OSU) URI, use the **config wlan hotspot hs2 osu sp uri delete** command.

config wlan hotspot hs2 osu sp uri delete *wlan-idosu-index*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
osu-index	OSU index. Enter a value between 1 and 16.

Command Default

The OSU URI is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to delete an OSU URI:

```
Cisco Controller > config wlan hotspot hs2 osu sp uri delete 12 2
```

config wlan hotspot hs2 wan-metrics downlink

To configure the downlink WAN metrics, use the **config wlan hotspot hs2 wan-metrics downlink** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
dlink-speed	WAN backhaul link speed, in Kbps. The range is from 0 to 4,294,967,295.
dlink-load	WAN backhaul link load. The range is from 0 to 100.

Command Default

The downlink WAN metrics are not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure downlink WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics downlink 12 2468 10
```

config wlan hotspot hs2 wan-metrics link-status

To configure the link status of WAN metrics, use the **config wlan hotspot hs2 wan-metrics link-status** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
link-status	Link status. Valid values are: • **0**—Unknown • **1**—Up • **2**—Down • **3**—Test

Command Default

The link status is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure the link status of WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics link-status 12 1
```

config wlan hotspot hs2 wan-metrics lmd

To configure the load measurement duration of WAN metrics, use the **config wlan hotspot hs2 wan-metrics lmd** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics lmd *wlan-id lmd-value*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
lmd-value	Load measurement duration of WAN. The range is from 0 to 65535.

Command Default

Load measurement duration of WAN is not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure load measurement duration of WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics lmd 1 2456
```

config wlan hotspot hs2 wan-metrics uplink

To configure the uplink WAN metrics, use the **config wlan hotspot hs2 wan-metrics uplink** command in WLAN configuration mode.

config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.
ulink-speed	WAN backhaul link speed, in Kbps. The range is from 0 to 4,294,967,295.
ulink-load	WAN backhaul link load. The range is from 0 to 100.

Command Default

The uplink WAN metrics are not configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to configure the uplink WAN metrics:

```
Cisco Controller > config wlan hotspot hs2 wan-metrics uplink 12 2468 10
```

config wlan hotspot msap

To configure the Mobility Service Advertisement Protocol (MSAP) parameters on a WLAN, use the **config wlan hotspot msap** command.

config wlan hotspot msap {**enable** | **disable** | **server-id** *server_id*} *wlan_id*

Syntax Description

enable	Enables MSAP on the WLAN.
disable	Disables MSAP on the WLAN.
server-id	Specifies the MSAP server id.
server_id	MSAP server ID. The range is from 1 to 10.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable MSAP on a WLAN:

```
(Cisco Controller) >config wlan hotspot msap enable 4
```

config wlan interface

To configure a wireless LAN interface or an interface group, use the **config wlan interface** command.

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

Syntax Description

wlan_id	(Optional) Wireless LAN identifier (1 to 512).
foreignAp	Specifies third-party access points.
interface-name	Interface name.
interface-group-name	Interface group name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an interface named VLAN901:

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

config wlan ipv6 acl

To configure IPv6 access control list (ACL) on a wireless LAN, use the **config wlan ipv6 acl** command.

config wlan ipv6 acl *wlan_id acl_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
acl_name	IPv6 ACL name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure an IPv6 ACL for local switching:

```
(Cisco Controller) >config wlan ipv6 acl 22 acl_sample
```

config wlan kts-cac

To configure the Key Telephone System-based CAC policy for a WLAN, use the **config wlan kts-cac** command.

config wlan kts-cac {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the KTS-based CAC policy.
disable	Disables the KTS-based CAC policy.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To enable the KTS-based CAC policy for a WLAN, ensure that you do the following:

- Configure the QoS profile for the WLAN to Platinum by entering the following command:

  config wlan qos *wlan-id* **platinum**

- Disable the WLAN by entering the following command:

  config wlan disable *wlan-id*

- Disable FlexConnect local switching for the WLAN by entering the following command:

  config wlan flexconnect local-switching *wlan-id* **disable**

The following example shows how to enable the KTS-based CAC policy for a WLAN with the ID 4:

```
(Cisco Controller) >config wlan kts-cac enable 4
```

config wlan layer2 acl

To configure a Layer 2 access control list (ACL) on a centrally switched WLAN, use the **config wlan acl layer2** command.

config wlan layer2 acl *wlan_id* { *acl_name* | **none** }

Syntax Description

wlan_id	Wireless LAN identifier. The range is from 1 to 512.
acl_name	Layer2 ACL name. The name can be up to 32 alphanumeric characters.
none	Clears any Layer2 ACL mapped to the WLAN.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can create a maximum of 16 rules for a Layer 2 ACL.

You can create a maximum of 64 Layer 2 ACLs on a controller.

A maximum of 16 Layer 2 ACLs are supported per access point because an access point supports a maximum of 16 WLANs.

s

Ensure that the Layer 2 ACL names do not conflict with the FlexConnect ACL names because an access point does not support the same Layer 2 and Layer 3 ACL names.

The following example shows how to apply a Layer 2 ACL on a WLAN:

```
(Cisco Controller) >config wlan layer2 acl 1 acl_l2_1
```

config wlan ldap

To add or delete a link to a configured Lightweight Directory Access Protocol (LDAP) server, use the **config wlan ldap** command.

config wlan ldap {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

Syntax Description

add	Adds a link to a configured LDAP server.
wlan_id	Wireless LAN identifier between 1 and 512.
server_id	LDAP server index.
delete	Removes the link to a configured LDAP server.
all	Specifies all LDAP servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use this command to specify the LDAP server priority for the WLAN.

To specify the LDAP server priority, one of the following must be configured and enabled:

- 802.1X authentication and Local EAP
- Web authentication and LDAP

Note Local EAP was introduced in controller software release 4.1; LDAP support on Web authentication was introduced in controller software release 4.2.

The following example shows how to add a link to a configured LDAP server with the WLAN ID 100 and server ID 4:

```
(Cisco Controller) >config wlan ldap add 100 4
```

config wlan learn-ipaddr-cswlan

To configure client IP address learning on a centrally switched WLAN, use the **config wlan learn-ipaddr-cswlan** command.

config wlan learn-ipaddr-cswlan *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
enable	Enables client IPv4 address learning on the centrally switched WLAN
disable	Disables client IPv4 address learning on the centrally switched WLAN

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

If the client is configured with Layer 2 encryption, the controller cannot learn the client IP address and will periodically drop the client. Disable this option so that the controller maintains the client connection without waiting to learn the client IP address.

The following example shows how to enable client IP address learning on a centrally switched WLAN:

```
(Cisco Controller) >config wlan learn-ipaddr-cswlan 2 enable
```

Related Commands

show wlan

config wlan load-balance

To override the global load balance configuration and enable or disable load balancing on a particular WLAN, use the **config wlan load-balance** command.

config wlan load-balance allow {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Load balancing is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable band selection on a wireless LAN with WLAN ID 3:

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

config wlan lobby-admin-access

To provide admin access to the lobby user on a particular WLAN, use the **config wlan lobby-admin-access** command.

config wlan lobby-admin-access {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables band selection on a wireless LAN.
disable	Disables band selection on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Lobby admin user is disabled by default.

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to enable lobby admin on a WLAN:

```
(Cisco Controller) >config wlan lobby-admin-access enable 2
```

config wlan mac-filtering

To change the state of MAC filtering on a wireless LAN, use the **config wlan mac-filtering** command.

config wlan mac-filtering {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables MAC filtering on a wireless LAN.
disable	Disables MAC filtering on a wireless LAN.
wlan_id	Wireless LAN identifier from 1 to 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the MAC filtering on WLAN ID 1:

```
(Cisco Controller) >config wlan mac-filtering enable 1
```

config wlan max-associated-clients

To configure the maximum number of client connections on a wireless LAN, guest LAN, or remote LAN, use the **config wlan max-associated-clients** command.

config wlan max-associated-clients *max_clients wlan_id*

Syntax Description

max_clients	Maximum number of client connections to be accepted.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections on WLAN ID 2:

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

config wlan max-radio-clients

To configure the maximum number of WLAN client per access point, use the **config wlan max-radio-clients** command.

config wlan max-radio-clients *max_radio_clients wlan_id*

Syntax Description

max_radio_clients	Maximum number of client connections to be accepted per access point radio. The valid range is from 1 to 200.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify the maximum number of client connections per access point radio on WLAN ID 2:

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

config wlan mdns

To configure an multicast DNS (mDNS) profile for a WLAN, use the **config wlan mdns** command.

config wlan mdns {**enable** | **disable** | **profile** {*profile-name* | **none**}} {*wlan_id* | **all**}

Syntax Description

enable	Enables mDNS snooping on a WLAN.
disable	Disables mDNS snooping on a WLAN.
profile	Configures an mDNS profile for a WLAN.
profile-name	Name of the mDNS profile to be associated with a WLAN.
none	Removes all existing mDNS profiles from the WLAN. You cannot configure mDNS profiles on the WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
all	Configures the mDNS profile for all WLANs.

Command Default

By default, mDNS snooping is enabled on WLANs.

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

You must disable the WLAN before you use this command. Clients receive service advertisements only for the services associated with the profile. The controller gives the highest priority to the profiles associated to interface groups, followed by the interface profiles, and then the WLAN profiles. Each client is mapped to a profile based on the order of priority.

The following example shows how to configure an mDNS profile for a WLAN.

```
(Cisco Controller) >config wlan mdns profile profile1 1
```

config wlan media-stream

To configure multicast-direct for a wireless LAN media stream, use the **config wlan media-stream** command.

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

Syntax Description

multicast-direct	Configures multicast-direct for a wireless LAN media stream.
wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all media streams.
enable	Enables global multicast to unicast conversion.
disable	Disables global multicast to unicast conversion.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Media stream multicast-direct requires load based Call Admission Control (CAC) to run. WLAN quality of service (QoS) needs to be set to either gold or platinum.

The following example shows how to enable the global multicast-direct media stream with WLAN ID 2:

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

config wlan mfp

To configure management frame protection (MFP) options for the wireless LAN, use the **config wlan mfp** command.

config wlan mfp {**client** [**enable** | **disable**] *wlan_id* | **infrastructure protection** [**enable** | **disable**] *wlan_id*}

Syntax Description

client	Configures client MFP for the wireless LAN.
enable	(Optional) Enables the feature.
disable	(Optional) Disables the feature.
wlan_id	Wireless LAN identifier (1 to 512).
infrastructure protection	(Optional) Configures the infrastructure MFP for the wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure client management frame protection for WLAN ID 1:

```
(Cisco Controller) >config wlan mfp client enable 1
```

config wlan mobility anchor

To change the state of MAC filtering on a wireless LAN, use the **config wlan mobility anchor** command.

config wlan mobility anchor {**add** | **delete**} *wlan_id ip_addr* **priority** *priority-number*

Syntax Description

add	Enables MAC filtering on a wireless LAN.
delete	Disables MAC filtering on a wireless LAN.
wlan_id	Wireless LAN identifier between 1 and 512.
ip_addr	Member switch IPv4 address for anchoring the wireless LAN.
priority	Sets priority to the anchored wireless LAN IP address.
priority-number	Range between 1 to 3.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.
8.1	**priority***priority number* parameter introduced.

The following example shows how to configure and set priority to the mobility wireless LAN anchor list with WLAN ID 4 and IPv4 address 192.168.0.14

```
(Cisco Controller) >config wlan mobility anchor add 4 192.168.0.14 priority 1
```

Related Commands

show wlan

config wlan mobility foreign-map

To configure interfaces or interface groups for foreign controllers, use the **config wlan mobility foreign-map** command.

config wlan mobility foreign-map {**add** | **delete**} *wlan_id foreign_mac_address* {*interface_name* | *interface_group_name*}

Syntax Description

add	Adds an interface or interface group to the map of foreign controllers.
delete	Deletes an interface or interface group from the map of foreign controllers.
wlan_id	Wireless LAN identifier from 1 to 512.
foreign_mac_address	Foreign switch MAC address on a WLAN.
interface_name	Interface name up to 32 alphanumeric characters.
interface_group_name	Interface group name up to 32 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an interface group for foreign controllers with WLAN ID 4 and a foreign switch MAC address on WLAN 00:21:1b:ea:36:60:

```
(Cisco Controller) >config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```

config wlan multicast buffer

To configure the radio multicast packet buffer size, use the **config wlan multicast buffer** command.

config wlan multicast buffer {**enable** | **disable**} *buffer-size*

Syntax Description

enable	Enables the multicast interface feature for a wireless LAN.
disable	Disables the multicast interface feature on a wireless LAN.
buffer-size	Radio multicast packet buffer size. The range is from 30 to 60. Enter 0 to indicate APs will dynamically adjust the number of buffers allocated for multicast.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default buffer size is 30

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure radio multicast buffer settings:

```
(Cisco Controller) >config wlan multicast buffer enable 45 222
```

config wlan multicast interface

To configure a multicast interface for a wireless LAN, use the **config wlan multicast interface** command.

config wlan multicast interface *wlan_id* {**enable** | **disable**} *interface_name*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
enable	Enables multicast interface feature for a wireless LAN.
delete	Disables multicast interface feature on a wireless LAN.
interface_name	Interface name. **Note** The interface name can only be specified in lower case characters.

Command Default

Multicast is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the multicast interface feature for a wireless LAN with WLAN ID 4 and interface name myinterface1:

```
(Cisco Controller) >config wlan multicast interface 4 enable myinterface1
```

config wlan mu-mimo

To enable Multi-User, Multiple-Input, Multiple-Output (MU-MIMO) on a WLAN, enter the **config wlan mu-mimo** command.

config wlan mu-mimo {**enable** | **disable**} *wlan-id*

Syntax Description

enable *wlan-id*	Enables MU-MIMO on the WLAN that is specified
disable *wlan-id*	Disables MU-MIMO on the WLAN that is specified

Command History

Release	Modification
8.1	This command was introduced.

config wlan nac

To enable or disable Network Admission Control (NAC) out-of-band support for a WLAN, use the **config wlan nac** command.

config wlan nac {**snmp** | **radius**} {**enable** | **disable**} *wlan_id*

Syntax Description

snmp	Configures SNMP NAC support.
radius	Configures RADIUS NAC support.
enable	Enables NAC for the WLAN.
disable	Disables NAC for the WLAN.
wlan_id	WLAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state. You also should disable FlexConnect local switching before you enable the RADIUS NAC state.

The following example shows how to configure SNMP NAC support for WLAN 13:

```
(Cisco Controller) >config wlan nac snmp enable 13
```

The following example shows how to configure RADIUS NAC support for WLAN 34:

```
(Cisco Controller) >config wlan nac radius enable 20
```

config wlan override-rate-limit

To override the bandwidth limits for upstream and downstream traffic per user and per service set identifier (SSID) defined in the QoS profile, use the **config wlan override-rate-limit** command.

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*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
average-data-rate	Specifies the average data rate for TCP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
average-realtime-rate	Specifies the average real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
burst-data-rate	Specifies the peak data rate for TCP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
burst-realtime-rate	Specifies the peak real-time data rate for UDP traffic per user or per SSID. The range is from 0 to 51,2000 Kbps.
per-ssid	Configures the rate limit for an SSID per radio. The combined traffic of all clients will not exceed this limit.
per-client	Configures the rate limit for each client associated with the SSID.
downstream	Configures the rate limit for downstream traffic.
upstream	Configures the rate limit for upstream traffic.
rate	Data rate for TCP or UDP traffic per user or per SSID. The range is form 0 to 51,2000 Kbps. A value of 0 imposes no bandwidth restriction on the QoS profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The rate limits are enforced by the controller and the AP. For central switching, the controller handles the downstream enforcement of per-client rate limit and the AP handles the enforcement of the upstream traffic and per-SSID rate limit for downstream traffic. When the AP enters standalone mode it handles the downstream enforcement of per-client rate limits too.

In FlexConnect local switching and standalone modes, per-client and per-SSID rate limiting is done by the AP for downstream and upstream traffic. However, in FlexConnect standalone mode, the configuration is not saved on the AP, so when the AP reloads, the configuration is lost and rate limiting does not happen after reboot.

For roaming clients, if the client roams between the APs on the same controller, same rate limit parameters are applied on the client. However, if the client roams from an anchor to a foreign controller, the per-client downstream rate limiting uses the parameters configured on the anchor controller while upstream rate limiting uses the parameters of the foreign controller.

The following example shows how to configure the burst real-time actual rate 2000 Kbps for the upstream traffic per SSID:

```
(Cisco Controller) >config wlan override-rate-limit 2 burst-realtime-rate per-ssid upstream
 2000
```

config wlan opendns-mode

To configure WLAN OpenDNS mode to force or copy or ignore the DNS to OpenDNS server access, use the **config wlan opendns-mode**command.

config wlan opendns-mode *wlan-id* { **ignore** | **force** | **copy** }

Syntax Description

wlan-id	Wireless LAN (WLAN) identifier.
ignore	Ignores the OpenDNS mode.
force	Forces the OpenDNS mode.
copy	Copies the OpenDNS mode.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to configure per WLAN OpenDNS mode to copy DNS to OpenDNS server:

```
(Cisco Controller) > config wlan opendns-mode wlan1 copy
```

config wlan opendns-profile

To configure per WLAN OpenDNS profile to force or copy or ignore the Domain Name System (DNS) to OpenDNS server access, use the **config wlan opendns-profile** command.

config wlan opendns profile *wlan-id profile-name* {**enable** | **disable**}

Syntax Description

wlan-id	Wireless LAN network.
profile-name	OpenDNS profile name used for tracking this profile.
enable	Maps OpenDNS identity.
disable	Removes OpenDNS identity.

Command Modes

(Controller Configuration) >

Command History

Release	Modification
8.4	This command was introduced.

Usage Guidelines

None

Example

The following example shows how to configure a WLAN on OpenDNS profile to force the DNS to OpenDNS server:

```
(Cisco Controller) > config wlan opendns-profile wlan1 user1 enable
```

config wlan passive-client

To configure passive-client feature on a wireless LAN, use the **config wlan passive-client** command.

config wlan passive-client {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the passive-client feature on a WLAN.
disable	Disables the passive-client feature on a WLAN.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You need to enable the global multicast mode and multicast-multicast mode by using the **config network multicast global** and **config network multicast mode** commands before entering this command.

Note You should configure the multicast in multicast-multicast mode only not in unicast mode. The passive client feature does not work with multicast-unicast mode in this release.

The following example shows how to configure the passive client on wireless LAN ID 2:

```
(Cisco Controller) >config wlan passive-client enable 2
```

config wlan peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **config wlan peer-blocking** command.

config wlan peer-blocking {**disable** | **drop** | **forward-upstream**} *wlan_id*

Syntax Description

disable	Disables peer-to-peer blocking and bridge traffic locally within the controller whenever possible.
drop	Causes the controller to discard the packets.
forward-upstream	Causes the packets to be forwarded on the upstream VLAN. The device above the controller decides what action to take regarding the packets.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the peer-to-peer blocking for WLAN ID 1:

```
(Cisco Controller) >config wlan peer-blocking disable 1
```

config wlan pmipv6 default-realm

To configure a default realm for a PMIPv6 WLAN, use the **config wlan pmipv6 default-realm** command.

config wlan pmipv6 default-realm { *default-realm-name* | **none** } *wlan_id*

Syntax Description

default-realm-name	Default realm name for the WLAN.
none	Clears the realm name for the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a default realm name on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```

config wlan pmipv6 mobility-type

To configure the mobility type on a WLAN, use the **config wlan pmipv6 mobility-type** command.

config wlan pmipv6 mobility-type { **none** | **pmipv6** } { *wlan_id* | **all** }

Syntax Description

none	Configures a WLAN with Simple IP mobility.
pmipv6	Configures a WLAN with PMIPv6 mobility.
all	Enables the specified type of mobility for all WLANs.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You must disable the WLAN when you configure the mobility type.

The following example shows how to configure the mobility type as PMIPv6 on a WLAN:

```
(Cisco Controller) >config wlan pmipv6 mobility-type pmipv6 16
```

config wlan pmipv6 profile_name

To configure a profile name for the PMIPv6 WLAN, use the **config wlan pmipv6 profile_name** command.

config wlan pmipv6 profile_name *profile_name wlan_id*

Syntax Description

profile_name	Profile name for the PMIPv6 WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command binds a profile name to the PMIPv6 WLAN or SSID. Each time that a mobile node associates with the controller, it uses the profile name and NAI in the trigger to the PMIPV6 module. The PMIPV6 module extracts all the profile specific parameters such as LMA IP, APN, and NAI and sends the PBU to the ASR5K.

The following example shows how to create a profile named ABC01 on a PMIPv6 WLAN:

```
(Cisco Controller) >config wlan pmipv6 profile_name ABC01 16
```

config wlan policy

To configure a policy on a WLAN, use the **config wlan policy** command.

config wlan policy {**add** | **delete**} *priority-index wlan-id*

Syntax Description

add	Adds a policy on a WLAN.
delete	Deletes an existing policy from a WLAN.
priority-index	Priority index of the policy to be configured on the WLAN. The policies are applied to the clients according to the priority index. The range is from 1 to 16.
policy_name	Name of the profiling policy.
wlan-id	WLAN identifier from 1 to 512.

Command Default

There is no WLAN policy.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

You can apply up to 16 policies on a WLAN.

The following example shows how to configure a policy on a WLAN:

```
(Cisco Controller) >config wlan policy add 1 teacher_policy 1
```

config wlan profiling

To configure client profiling on a WLAN, use the **config wlan profiling** command.

config wlan profiling { **local** | **radius** } { **all** | **dhcp** | **http** } { **enable** | **disable** } *wlan_id*

Syntax Description

local	Configures client profiling in Local mode for a WLAN.
radius	Configures client profiling in RADIUS mode on a WLAN.
all	Configures DHCP and HTTP client profiling in a WLAN.
dhcp	Configures DHCP client profiling alone in a WLAN.
http	Configures HTTP client profiling in a WLAN.
enable	Enables the specific type of client profiling in a WLAN. When you enable HTTP profiling, the controller collects the HTTP attributes of clients for profiling. When you enable DHCP profiling, the controller collects the DHCP attributes of clients for profiling.
disable	Disables the specific type of client profiling in a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Usage Guidelines

Ensure that you have disabled the WLAN before configuring client profiling on the WLAN.

Command Default

Client profiling is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Only clients connected to port 80 for HTTP can be profiled. IPv6 only clients are not profiled.

If a session timeout is configured for a WLAN, clients must send the HTTP traffic before the configured timeout to get profiled.

This feature is not supported on the following:

- FlexConnect Standalone mode
- FlexConnect Local Authentication

The following example shows how to enable both DHCP and HTTP profiling on a WLAN:

```
(Cisco Controller) >config wlan profiling radius all enable 6
                                        HTTP Profiling successfully enabled.
                                        DHCP Profiling successfully enabled.
```

config wlan qos

To change the quality of service (QoS) for a wireless LAN, use the **config wlan qos** command.

config wlan qos *wlan_id* {**bronze** | **silver** | **gold** | **platinum**}
config wlan qos foreignAp {**bronze** | **silver** | **gold** | **platinum**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
bronze	Specifies the bronze QoS policy.
silver	Specifies the silver QoS policy.
gold	Specifies the gold QoS policy.
platinum	Specifies the platinum QoS policy.
foreignAp	Specifies third-party access points.

Command Default

The default QoS policy is silver.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the highest level of service on wireless LAN 1:

```
(Cisco Controller) >config wlan qos 1 gold
```

config wlan radio

To set the Cisco radio policy on a wireless LAN, use the **config wlan radio** command.

config wlan radio *wlan_id* {**all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
all	Configures the wireless LAN on all radio bands.
802.11a	Configures the wireless LAN on only 802.11a.
802.11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled).
802.11g	Configures the wireless LAN on 802.11g only.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the wireless LAN on all radio bands:

```
(Cisco Controller) >config wlan radio 1 all
```

config wlan radius_server acct

To configure RADIUS accounting servers of a WLAN, use the **config wlan radius_server acct** command.

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*}

Syntax Description

enable	Enables RADIUS accounting for the WLAN.
disable	Disables RADIUS accounting for the WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
add	Adds a link to a configured RADIUS accounting server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS accounting server.
address	Configures an accounting framed IPv6 attribute to an IPv6 address.
both	Configures the accounting framed IPv6 attribute to an IPv6 address and prefix.
prefix	Configures the accounting framed IPv6 attribute to an IPv6 prefix.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable RADIUS accounting for the WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

The following example shows how to add a link to a configured RADIUS accounting server:

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

config wlan radius_server acct interim-update

To configure the interim update of a RADIUS accounting server of a WLAN, use the **config wlan radius_server acct interim-update** command.

config wlan radius_server acct interim-update {**enable** | **disable** | *interval* } *wlan_id*

Syntax Description

interim-update	Configures the interim update of the RADIUS accounting server.
enable	Enables interim update of the RADIUS accounting server for the WLAN.
disable	Disables interim update of the RADIUS accounting server for the WLAN.
interval	Interim update interval that you specify. The valid range is 180 seconds to 3600 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Interim update of a RADIUS accounting sever is set at 600 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify an interim update of 200 seconds to a RADIUS accounting server of WLAN 2:

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan radius_server auth

To configure RADIUS authentication servers of a WLAN, use the **config wlan radius_server auth** command.

config wlan radius_server auth {**enable** *wlan_id* | **disable** *wlan_id*} {**add** *wlan_id server_id* | **delete** *wlan_id* {**all** | *server_id*}}

Syntax Description

auth	Configures a RADIUS authentication
enable	Enables RADIUS authentication for this WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.
disable	Disables RADIUS authentication for this WLAN.
add	Adds a link to a configured RADIUS server.
server_id	RADIUS server index.
delete	Deletes a link to a configured RADIUS server.
all	Deletes all links to configured RADIUS servers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a link to a configured RADIUS authentication server with WLAN ID 1 and Server ID 1:

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

config wlan radius_server overwrite-interface

To configure a wireless LAN's RADIUS dynamic interface, use the **config wlan radius_server overwrite-interface** command.

config wlan radius_server overwrite-interface {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables RADIUS dynamic interface for this WLAN.
disable	Disables RADIUS dynamic interface for this WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The controller uses the management interface as identity. If the RADIUS server is on a directly connected dynamic interface, the traffic is sourced from the dynamic interface. Otherwise, the management IP address is used.

If the feature is enabled, controller uses the interface specified on the WLAN configuration as identity and source for all RADIUS related traffic on the WLAN.

The following example shows how to enable RADIUS dynamic interface for a WLAN with an ID 1:

```
(Cisco Controller) >config wlan radius_server overwrite-interface enable 1
```

config wlan radius_server realm

To configure realm on a WLAN, use the **config wlan radius_server realm** command.

config wlan *radius_server***realm** {**enable** | **disable**} *wlan-id*

Syntax Description

radius_server	Radius server index. The range is from 1 to 17.
enable	Enable realm on a WLAN.
disable	Disable realm on a WLAN.
wlan-id	WLAN ID. The range is from 1 to 512.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to enable realm on a WLAN:

```
(Cisco Controller) > config wlan 2 realm enable 50
```

config wlan roamed-voice-client re-anchor

To configure a roamed voice client's reanchor policy, use the **config wlan roamed-voice-client re-anchor** command.

config wlan roamed-voice-client re-anchor {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the roamed client's reanchor policy.
disable	Disables the roamed client's reanchor policy.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The roamed client reanchor policy is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a roamed voice client's reanchor policy where WLAN ID is 1:

```
(Cisco Controller) >config wlan roamed-voice-client re-anchor enable 1
```

config wlan security 802.1X

To change the state of 802.1X security on the wireless LAN Cisco radios, use the **config wlan security 802.1X** command.

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**}}

Syntax Description

enable	Enables the 802.1X settings.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
disable	Disables the 802.1X settings.
encryption	Specifies the static WEP keys and indexes.
0	Specifies a WEP key size of 0 (no encryption) bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
40	Specifies a WEP key size of 40 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
104	Specifies a WEP key size of 104 bits. The default value is 104. **Note** All keys within a wireless LAN must be the same size.
on-macfilter-failure	Configures 802.1X on MAC filter failure.
enable	Enables 802.1X authentication on MAC filter failure.
disable	Disables 802.1X authentication on MAC filter failure.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To change the encryption level of 802.1X security on the wireless LAN Cisco radios, use the following key sizes:

- 0—no 802.1X encryption.
- 40—40/64-bit encryption.

- 104—104/128-bit encryption. (This is the default encryption setting.)

The following example shows how to configure 802.1X security on WLAN ID 16.

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

config wlan security ckip

To configure Cisco Key Integrity Protocol (CKIP) security options for the wireless LAN, use the **config wlan security ckip** command.

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*]

Syntax Description

enable	Enables CKIP security.
disable	Disables CKIP security.
wlan_id	Wireless LAN identifier from 1 to 512.
akm psk set-key	(Optional) Configures encryption key management for the CKIP wireless LAN.
hex	Specifies a hexadecimal encryption key.
ascii	Specifies an ASCII encryption key.
40	Sets the static encryption key length to 40 bits for the CKIP WLAN. 40-bit keys must contain 5 ASCII text characters or 10 hexadecimal characters.
104	Sets the static encryption key length to 104 bits for the CKIP WLAN. 104-bit keys must contain 13 ASCII text characters or 26 hexadecimal characters.
key	Specifies the CKIP WLAN key settings.
key_index	Configured PSK key index.
mmh-mic	(Optional) Configures multi-modular hash message integrity check (MMH MIC) validation for the CKIP wireless LAN.
kp	(Optional) Configures key-permutation for the CKIP wireless LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a CKIP WLAN encryption key of 104 bits (26 hexadecimal characters) for PSK key index 2 on WLAN 03:

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

config wlan security cond-web-redir

To enable or disable conditional web redirect, use the **config wlan security cond-web-redir** command.

config wlan security cond-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables conditional web redirect.
disable	Disables conditional web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the conditional web direct on WLAN ID 2:

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```

config wlan security eap-params

To configure local EAP timers on a WLAN, use the **config wlan security eap-params** command.

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*

Syntax Description

{**enable** | **disable** }	Specifies to enable or disable SSID specific EAP timeouts or retries. The default value is disabled.
eapol-key-timeout *timeout*	Specifies the amount of time (200 to 5000 milliseconds) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The valid range is 200 to 5000 milliseconds. The default value is 1000 milliseconds.
eapol-key-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to send an EAP key over the WLAN to wireless clients using local EAP. The default value is 2.
identity-request- timeout *timeout*	Specifies the amount of time (1 to 120 seconds) that the controller attempts to send an EAP identity request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
identity-request-retries *retries*	Specifies the maximum number of times (0 to 4 retries) that the controller attempts to retransmit the EAP identity request to wireless clients within WLAN using local EAP. The default value is 2.
request-timeout	Specifies the amount of time (1 to 120 seconds) in which the controller attempts to send an EAP parameter request to wireless clients within WLAN using local EAP. The default value is 30 seconds.
request-retries*retries*	Specifies the maximum number of times (0 to 20 retries) that the controller attempts to retransmit the EAP parameter request to wireless clients within WLAN using local EAP. The default value is 2.
wlan-id	WLAN identification number.

Command Default

The default EAPOL key timeout is 1000 milliseconds.

The default for EAPOL key retries is 2.

The default identity request timeout is 30 seconds.

The default identity request retries is 2.

The default request timeout is 30 seconds.

The default request retries is 2.

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to enable SSID specific EAP parameters on a WLAN:

```
(Cisco Controller) > config wlan security eap-params enable 4
```

The following example shows how to set EAPOL key timeout parameter on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

The following example shows how to set EAPOL key retries on a WLAN:

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

config wlan security eap-passthru

To configure the 802.1X frames pass through on to the external authenticator, use the **config wlan security eap-passthru** command.

config wlan security eap-passthru {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.1X frames pass through to external authenticator.
disable	Disables 802.1X frames pass through to external authenticator.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the 802.1X frames pass through to external authenticator on WLAN ID 2:

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

config wlan security ft {**adaptive** | **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

adaptive	Configures 802.11r Fast Transition Roaming adaptive support. This is the default option.
enable	Enables 802.11r Fast Transition Roaming support.
disable	Disables 802.11r Fast Transition Roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was modified. The **adaptive** keyword was added.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security ft over-the-ds

To configure 802.11r fast transition parameters over a distributed system, use the **config wlan security ft over-the-ds** command.

config wlan security ft over-the-ds {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables 802.11r fast transition roaming support over a distributed system.
disable	Disables 802.11r fast transition roaming support over a distributed system.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

Ensure that 802.11r fast transition is enabled on the WLAN.

The following example shows how to enable 802.11r fast transition roaming support over a distributed system on WLAN ID 2:

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

config wlan security IPsec disable

To disable IPsec security, use the **config wlan security IPsec disable** command.

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec disable 16
```

config wlan security IPsec enable

To enable IPsec security, use the **config wlan security IPsec enable** command.

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the IPsec for WLAN ID 16:

```
(Cisco Controller) >config wlan security IPsec enable 16
```

config wlan security IPsec authentication

To modify the IPsec security authentication protocol used on the wireless LAN, use the **config wlan security IPsec authentication** command.

config wlan security IPsec authentication {**hmac-md5** | **hmac-sha-1**} {*wlan_id* | **foreignAp**}

Syntax Description

hmac-md5	Specifies the IPsec HMAC-MD5 authentication protocol.
hmac-sha-1	Specifies the IPsec HMAC-SHA-1 authentication protocol.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec HMAC-SHA-1 security authentication parameter for WLAN ID 1:

```
(Cisco Controller) >config wlan security IPsec authentication hmac-sha-1 1
```

config wlan security IPsec encryption

To modify the IPsec security encryption protocol used on the wireless LAN, use the **config wlan security IPsec encryption** command.

config wlan security IPsec encryption {**3des** | **aes** | **des**} {*wlan_id* | **foreignAp**}

Syntax Description

3des	Enables IPsec 3DES encryption.
aes	Enables IPsec AES 128-bit encryption.
des	Enables IPsec DES encryption.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec AES encryption:

```
(Cisco Controller) >config wlan security IPsec encryption aes 1
```

config wlan security IPsec config

To configure the proprietary Internet Key Exchange (IKE) CFG-Mode parameters used on the wireless LAN, use the **config wlan security IPsec config** command.

config wlan security IPsec config qotd *ip_address* {*wlan_id* | **foreignAp**}

Syntax Description

qotd	Configures the quote-of-the day server IP for cfg-mode.
ip_address	Quote-of-the-day server IP for cfg-mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

IKE is used as a method of distributing the session keys (encryption and authentication), as well as providing a way for the VPN endpoints to agree on how the data should be protected. IKE keeps track of connections by assigning a bundle of Security Associations (SAs), to each connection.

The following example shows how to configure the quote-of-the-day server IP 44.55.66.77 for cfg-mode for WLAN 1:

```
(Cisco Controller) >config wlan security IPsec config qotd 44.55.66.77 1
```

config wlan security IPsec ike authentication

To modify the IPsec Internet Key Exchange (IKE) authentication protocol used on the wireless LAN, use the **config wlan security IPsec ike authentication** command.

config wlan security IPsec ike authentication {**certificates** {*wlan_id* | **foreignAp**} | **pre-share-key** {*wlan_id* | **foreignAp**} *key* | **xauth-psk** {*wlan_id* | **foreignAp**} *key*}

Syntax Description

certificates	Enables the IKE certificate mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
pre-share-key	Enables the IKE Xauth with preshared keys.
xauth-psk	Enables the IKE preshared key.
key	Key required for preshare and xauth-psk.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IKE certification mode:

```
(Cisco Controller) >config wlan security IPsec ike authentication certificates 16
```

config wlan security IPsec ike dh-group

To modify the IPsec Internet Key Exchange (IKE) Diffie Hellman group used on the wireless LAN, use the **config wlan security IPsec ike dh-group** command.

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
group-1	Specifies DH group 1 (768 bits).
group-2	Specifies DH group 2 (1024 bits).
group-5	Specifies DH group 5 (1536 bits).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the Diffe Hellman group parameter for group-1:

```
(Cisco Controller) >config wlan security IPsec ike dh-group 1 group-1
```

config wlan security IPsec ike lifetime

To modify the IPsec Internet Key Exchange (IKE) lifetime used on the wireless LAN, use the **config wlan security IPsec ike lifetime** command.

config wlan security IPsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
seconds	IKE lifetime in seconds, between 1800 and 345600.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the IPsec IKE lifetime use on the wireless LAN:

```
(Cisco Controller) >config wlan security IPsec ike lifetime 1 1900
```

config wlan security IPsec ike phase1

To modify IPsec Internet Key Exchange (IKE) Phase 1 used on the wireless LAN, use the **config wlan security IPsec ike phase1** command.

config wlan security IPsec ike phase1 {**aggressive** | **main**} {*wlan_id* | **foreignAp**}

Syntax Description

aggressive	Enables the IKE aggressive mode.
main	Enables the IKE main mode.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec IKE Phase 1:

```
(Cisco Controller) >config wlan security IPsec ike phase1 aggressive 16
```

config wlan security IPsec ike contivity

To modify Nortel's Contivity VPN client support on the wireless LAN, use the **config wlan security IPsec ike contivity** command.

config wlan security IPsec ike contivity {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

enable	Enables contivity support for this WLAN.
disable	Disables contivity support for this WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify Contivity VPN client support:

```
(Cisco Controller) >config wlan security IPsec ike contivity enable 14
```

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security ft

To configure 802.11r Fast Transition Roaming parameters, use the **config wlan security ft** command.

config wlan security ft {**adaptive** | **enable** | **disable** | **reassociation-timeout** *timeout-in-seconds*} *wlan_id*

Syntax Description

adaptive	Configures 802.11r Fast Transition Roaming adaptive support. This is the default option.
enable	Enables 802.11r Fast Transition Roaming support.
disable	Disables 802.11r Fast Transition Roaming support.
reassociation-timeout	Configures reassociation deadline interval.
timeout-in-seconds	Reassociation timeout value, in seconds. The valid range is 1 to 100 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was modified. The **adaptive** keyword was added.

Usage Guidelines

Ensure that you have disabled the WLAN before you proceed.

The following example shows how to enable 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft enable 2
```

The following example shows how to set a reassociation timeout value of 20 seconds for 802.11r Fast Transition Roaming support on WLAN 2:

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security passthru

To modify the IPsec pass-through used on the wireless LAN, use the **config wlan security passthru** command.

config wlan security passthru {**enable** | **disable**} {*wlan_id* | **foreignAp**} [*ip_address*]

Syntax Description

enable	Enables IPsec pass-through.
disable	Disables IPsec pass-through.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
ip_address	(Optional) IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to modify IPsec pass-through used on the wireless LAN:

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

config wlan security pmf

To configure 802.11w Management Frame Protection (MFP) on a WLAN, use the **config wlan security pmf** command.

config wlan security pmf {**disable** | **optional** | **required** | **association-comeback** *association-comeback_timeout* | **saquery-retrytimeout** *saquery-retry_timeout*} *wlan_id*

Syntax Description

disable	Disables 802.11w MFP protection on a WLAN.
optional	Enables 802.11w MFP protection on a WLAN.
required	Requires clients to negotiate 802.11w MFP protection on a WLAN.
association-comeback	Configures the 802.11w association comeback time.
association-comeback_timeout	Association comeback interval in seconds. Time interval that an associated client must wait before the association is tried again after it is denied with a status code 30. The status code 30 message is "Association request rejected temporarily; Try again later". The range is from 1 to 20 seconds.
saquery-retrytimeout	Configures the 802.11w Security Association (SA) query retry timeout.
saquery-retry_timeout	Time interval identified in the association response to an already associated client before the association can be tried again. This time interval checks if the client is a real client and not a rogue client during the association comeback time. If the client does not respond within this time, the client association is deleted from the controller. The range is from 100 to 500 ms.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Default SA query retry timeout is 200 milliseconds.

Default association comeback timeout is 1 second.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

802.11w introduces an Integrity Group Temporal Key (IGTK) that is used to protect broadcast or multicast robust management frames. IGTK is a random value, assigned by the authenticator station (controller) used to protect MAC management protocol data units (MMPDUs) from the source STA. The 802.11w IGTK key is derived using the four way handshake and is used only on WLANs that are configured with WPA or WPA2 security at Layer 2.

The following example shows how to enable 802.11w MFP protection on a WLAN:

```
(Cisco Controller) > config wlan security pmf optional 1
```

The following example shows how to configure the SA query retry timeout on a WLAN:

```
(Cisco Controller) > config wlan security pmf saquery-retrytimeout 300 1
```

config wlan security sgt

To configures Secure Group Tag (SGT) for a WLAN, use the **config wlan security sgt** command.

config wlan security sgt {*value* | *wlan-id*} *wlan_id*

Syntax Description

value	SGT value
wlan-id	WLAN ID

Command Default

None

Command History

Release	Modification
8.4	This command was introduced

config wlan security splash-page-web-redir

To enable or disable splash page web redirect, use the **config wlan security splash-page-web-redir** command.

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables splash page web redirect.
disable	Disables splash page web redirect.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Splash page web redirect is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable spash page web redirect:

```
(Cisco Controller) >config wlan security splash-page-web-redir enable 2
```

config wlan security static-wep-key authentication

To configure static Wired Equivalent Privacy (WEP) key 802.11 authentication on a wireless LAN, use the **config wlan security static-wep-key authentication** command.

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

Syntax Description

shared-key	Enables shared key authentication.
open	Enables open system authentication.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the static WEP shared key authentication for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

config wlan security static-wep-key disable

To disable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key disable** command.

config wlan security static-wep-key disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable the static WEP keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

config wlan security static-wep-key enable

To enable the use of static Wired Equivalent Privacy (WEP) keys, use the **config wlan security static-wep-key enable** command.

config wlan security static-wep-key enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the use of static WEK keys for WLAN ID 1:

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```

config wlan security static-wep-key encryption

To configure the static Wired Equivalent Privacy (WEP) keys and indexes, use the **config wlan security static-wep-key encryption** command.

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
40	Specifies the encryption level of 40.
104	Specifies the encryption level of 104.
hex	Specifies to use hexadecimal characters to enter key.
ascii	Specifies whether to use ASCII characters to enter key.
key	WEP key in ASCII.
key-index	Key index (1 to 4).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

One unique WEP key index can be applied to each wireless LAN. Because there are only four WEP key indexes, only four wireless LANs can be configured for static WEP Layer 2 encryption.

Make sure to disable 802.1X before using this command.

The following example shows how to configure the static WEP keys for WLAN ID 1 that uses hexadecimal character 0201702001 and key index 2:

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001 2
```

config wlan security tkip

To configure the Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) countermeasure hold-down timer, use the **config wlan security tkip** command.

config wlan security tkip hold-down *time wlan_id*

Syntax Description

hold-down	Configures the TKIP MIC countermeasure hold-down timer.
time	TKIP MIC countermeasure hold-down time in seconds. The range is from 0 to 60 seconds.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

The default TKIP countermeasure is set to 60 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

TKIP countermeasure mode can occur if the access point receives 2 MIC errors within a 60 second period. When this situation occurs, the access point deauthenticates all TKIP clients that are associated to that 802.11 radio and holds off any clients for the countermeasure holdoff time.

The following example shows how to configure the TKIP MIC countermeasure hold-down timer:

```
(Cisco Controller) >config wlan security tkip
```

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

timeout	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default client session idle timeout is 300 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan security web-auth

To change the status of web authentication used on a wireless LAN, use the **config wlan security web-auth** command.

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* }}

Syntax Description

acl	Configures the access control list.
enable	Enables web authentication.
disable	Disables web authentication.
wlan_id	Wireless LAN identifier from 1 to 512.
foreignAp	Specifies third-party access points.
acl_name	(Optional) ACL name (up to 32 alphanumeric characters).
none	(Optional) Specifies no ACL name.
on-macfilter-failure	Enables web authentication on MAC filter failure.
server-precendence	Configures the authentication server precedence order for Web-Auth users.
local	Specifies the server type.
ldap	Specifies the server type.
radius	Specifies the server type.
flexacl	Configures Flexconnect Access Control List.
ipv4_acl_name	(Optional) IPv4 ACL name. You can enter up to 32 alphanumeric characters.
ipv6_acl_name	(Optional) IPv6 ACL name. You can enter up to 32 alphanumeric characters.
ipv6	Configures IPv6 related parameters.
mac-auth-server	Configures MAC authentication server for the WLAN.

timeout	Configures Local Web authentication Timeout. **Note** The CWA session timeout is fixed to 600 seconds.
value_in_seconds	Timeout value in seconds; valid range is between 300 and 14400 seconds.
web-portal-server	Configures CMCC web portal server for the WLAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the security policy for WLAN ID 1 and an ACL named ACL03:

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```

config wlan security web-auth captive-bypass

To configure captive-bypass on a wireless LAN, use the **config wlan security web-auth captive-bypass** command.

config wlan security web-auth captive-bypass {**enable | disable | none** }

Syntax Description

enable	Enable the captive-bypass for WLAN.
disable	Disable the captive-bypass for WLAN.
none	Clear the captive-bypass configuration for WLAN. And global captive netwrok assistant bypass setting will get applied
wlan-id	Enter WLAN identifier between 1 and 16.

Command History

Release	Modification
8.4	This command is introduced.

The following example shows how to enable Captive Network Bypass:

```
(Cisco Controller) >config wlan security web-auth captive-bypass enable 1
```

config wlan security web-auth qrscan-des-key

To configure the QR-scan DES key in a WLAN, use the **config wlan security web-auth qrscan-des-key** command.

config wlan security web-auth qrscan-des-key {*DES key stringwlan_id* }

Syntax Description

DES key string	Enter the DES key of 8 characters.
wlan-id	Enter WLAN Identifier between 1 and 16.

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to configure the QR-scan DES key:

```
(Cisco Controller) >config wlan security web-auth qrscan-des-key 1
```

config wlan security web-passthrough acl

To add an access control list (ACL) to the wireless LAN definition, use the **config wlan security web-passthrough acl** command.

config wlan security web-passthrough acl {*wlan_id* | **foreignAp**} {*acl_name* | **none**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
acl_name	ACL name (up to 32 alphanumeric characters).
none	Specifies that there is no ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add an ACL to the wireless LAN definition:

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```

config wlan security web-passthrough disable

To disable a web captive portal with no authentication required on a wireless LAN, use the **config wlan security web-passthrough disable** command.

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

config wlan security web-passthrough email-input

To configure a web captive portal using an e-mail address, use the **config wlan security web-passthrough email-input** command.

config wlan security web-passthrough email-input {**enable** | **disable**} {*wlan_id* | **foreignAp**}

Syntax Description

email-input	Configures a web captive portal using an e-mail address.
enable	Enables a web captive portal using an e-mail address.
disable	Disables a web captive portal using an e-mail address.
wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure a web captive portal using an e-mail address:

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

config wlan security web-passthrough enable

To enable a web captive portal with no authentication required on the wireless LAN, use the **config wlan security web-passthrough enable** command.

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a web captive portal with no authentication required on wireless LAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

config wlan security web-passthrough qr-scan

To enable or disable qr-scan on the WLAN, use the **config wlan security web-passthrough qr-scan** command.

config wlan security web-passthrough qr-scan { { **localenable | disable** } | **enable | disable** }

Syntax Description

local	Configures QR code scanning support locally on AP for clients. • **enable**–enables QR code scanning support for clients. • **disable**–disables QR code scanning support for clients.
enable	Enables QR code scanning support for clients.
disable	Disables QR code scanning support for clients.
wlan-id	Enter WLAN Identifier between 1 and 16.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

The following example shows how to enable qr-scan on WLAN ID 1:

```
(Cisco Controller) >config wlan security web-passthrough qr-scan enable 1
```

config wlan security wpa akm 802.1x

To configure authentication key-management (AKM) using 802.1X, use the **config wlan security wpa akm 802.1x** command.

config wlan security wpa akm 802.1x {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the 802.1X support.
disable	Disables the 802.1X support.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication using 802.1X.

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

config wlan security wpa akm cckm

To configure authentication key-management using Cisco Centralized Key Management (CCKM), use the **config wlan security wpa akm cckm** command.

config wlan security wpa akm cckm { **enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

Syntax Description

enable	Enables CCKM support.
disable	Disables CCKM support.
wlan_id	Wireless LAN identifier between 1 and 512.
timestamp-tolerance	CCKM IE time-stamp tolerance. The range is between 1000 to 5000 milliseconds; the default is 1000 milliseconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using CCKM.

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

config wlan security wpa akm ft

To configure authentication key-management using 802.11r fast transition 802.1X, use the **config wlan security wpa akm ft** command.

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout** *seconds*]] {**enable** | **disable**} *wlan_id*

Syntax Description

over-the-air	(Optional) Configures 802.11r fast transition roaming over-the-air support.
over-the-ds	(Optional) Configures 802.11r fast transition roaming DS support.
psk	(Optional) Configures 802.11r fast transition PSK support.
reassociation-timeout	(Optional) Configures the reassociation deadline interval. The valid range is between 1 to 100 seconds. The default value is 20 seconds.
seconds	Reassociation deadline interval in seconds.
enable	Enables 802.11r fast transition 802.1X support.
disable	Disables 802.11r fast transition 802.1X support.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure authentication key-management using 802.11r fast transition:

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security wpa akm pmf

To configure Authenticated Key Management (AKM) of management frames, use the **config wlan security wpa akm pmf** command.

config wlan security wpa akm pmf {**802.1x** | **psk**} {**enable** | **disable**} *wlan_id*

Syntax Description

802.1x	Configures 802.1X authentication for protection of management frames (PMF).
psk	Configures preshared keys (PSK) for PMF.
enable	Enables 802.1X authentication or PSK for PMF.
disable	Disables 802.1X authentication or PSK for PMF.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

802.11w has two new AKM suites: 00-0F-AC:5 or 00-0F-AC:6. You must enable WPA and then disable the WLAN to configure PMF on the WLAN.

The following example shows how to enable 802.1X authentication for PMF in a WLAN:

```
(Cisco Controller) >config wlan security wpa akm pmf 802.1x enable 1
```

config wlan security wpa akm psk

To configure the Wi-Fi protected access (WPA) preshared key mode, use the **config wlan security wpa akm psk** command.

config wlan security wpa akm psk { { **enable** | **disable** } | { **set-key** *key-format key* } | { **auto-key** { **enable** | **disable** } } | { **pmkid** { **enable** | **disable** } } *wlan_id* }

Syntax Description

enable	Enables WPA-PSK.
disable	Disables WPA-PSK.
set-key	Configures a preshared key.
key-format	Specifies key format. Either ASCII or hexadecimal.
key	WPA preshared key.
auto-key {**enable** | **disable**}	Configures auto PSK on the WLAN.
pmkid {**enable** | **disable**}	Configures PMK ID inclusion in M1 of 4-way handshake messages.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.10	The **pmkid** {**enable** | **disable**} was introduced.

Examples

The following example shows how to configure the WPA preshared key mode:

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

config wlan security wpa disable

To disable WPA1, use the **config wlan security wpa disable** command.

config wlan security wpa disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA:

```
(Cisco Controller) >config wlan security wpa disable 1
```

config wlan security wpa enable

To enable WPA1, use the **config wlan security wpa enable** command.

config wlan security wpa enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the WPA on WLAN ID 1:

```
(Cisco Controller) >config wlan security wpa enable 1
```

config wlan security wpa ciphers

To configure the Wi-Fi protected authentication (WPA1) or Wi-Fi protected authentication (WPA2), use the **config wlan security wpa ciphers** command.

config wlan security wpa {**wpa1** | **wpa2**} **ciphers** {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

wpa1	Configures WPA1 support.
wpa2	Configures WPA2 support.
ciphers	Configures WPA ciphers.
aes	Configures AES encryption support.
tkip	Configures TKIP encryption support.
enable	Enables WPA AES/TKIP mode.
disable	Disables WPA AES/TKIP mode.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you are not specifying the WPA versions, it implies the following:

- If the cipher enabled is AES, you are configuring WPA2/AES.
- If the ciphers enabled is AES+TKIP, you are configuring WPA/TKIP, WPA2/AES,or WPA/TKIP.
- If the cipher enabled is TKIP, you are configuring WPA/TKIP or WPA2/TKIP.

The following example shows how to encrypt the WPA:

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

config wlan security wpa gtk-random

To enable the randomization of group temporal keys (GTK) between access points and clients on a WLAN, use the **config wlan security wpa gtk-random** command.

config wlan security wpa gtk-random {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables the randomization of GTK keys between the access point and clients.
disable	Disables the randomization of GTK keys between the access point and clients.
wlan_id	WLAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you enable this command, the clients in the Basic Service Set (BSS) get a unique GTK key. The clients do not receive multicast or broadcast traffic.

The following example shows how to enable the GTK randomization for each client associated on a WLAN:

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

config wlan security wpa osen disable

To disable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen disable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default

OSEN is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to disable OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen disable 12
```

config wlan security wpa osen enable

To enable OSU Server-Only Authenticated L2 Encryption Network (OSEN) on a WLAN, use the **config wlan security wpa osen enable** command in WLAN configuration mode.

config wlan security wpa osen enable *wlan-id*

Syntax Description

wlan-id	WLAN identification number. Enter a value between 1 and 512.

Command Default

OSEN is not enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

This example shows how to enable an OSEN on a WLAN:

```
Cisco Controller > config wlan security wpa osen enable 12
```

config wlan security wpa wpa1 disable

To disable WPA1, use the **config wlan security wpa wpa1 disable** command.

config wlan security wpa wpa1 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```

config wlan security wpa wpa1 enable

To enable WPA1, use the **config wlan security wpa wpa1 enable** command.

config wlan security wpa wpa1 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

config wlan security wpa wpa2 disable

To disable WPA2, use the **config wlan security wpa wpa2 disable** command.

config wlan security wpa wpa2 disable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```

config wlan security wpa wpa2 enable

To enable WPA2, use the **config wlan security wpa wpa2 enable** command.

config wlan security wpa wpa2 enable *wlan_id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

config wlan security wpa wpa2 cache

To configure caching methods on a WLAN, use the **config wlan security wpa wpa2 cache** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

sticky	Configures Sticky Key Caching (SKC) roaming support on the WLAN.
enable	Enables SKC roaming support on the WLAN.
disable	Disables SKC roaming support on the WLAN.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

In SKC (Sticky Key caching) also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has a PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs.

The following example shows how to enable SKC roaming support on a WLAN:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

config wlan security wpa wpa2 cache sticky

To configure Sticky PMKID Caching (SKC) on a WLAN, use the **config wlan security wpa wpa2 cache sticky** command.

config wlan security wpa wpa2 cache sticky {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables SKC on a WLAN.
disable	Disables SKC on a WLAN.
wlan_id	Wireless LAN identifier between 1 and 512 (inclusive).

Command Default

Stkcky PMKID Caching is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Beginning in Release 7.2 and later releases, the controller supports Sticky PMKID Caching (SKC). With sticky PMKID caching, the client receives and stores a different PMKID for every AP it associates with. The APs also maintain a database of the PMKID issued to the client. In SKC also known as PKC (Pro Active Key caching), the client stores each Pairwise Master Key (PMK) ID (PMKID) against a Pairwise Master Key Security Association (PMKSA). When a client finds an AP for which it has the PMKSA, it sends the PMKID in the association request to the AP. If the PMKSA is alive in the AP, the AP provides support for fast roaming. In SKC, full authentication is done on each new AP to which the client associates and the client must keep the PMKSA associated with all APs. For SKC, PMKSA is a per AP cache that the client stores and PMKSA is precalculated based on the BSSID of the new AP.

- You cannot use SKC for large scale deployments as the controller supports SKC only up to eight APs.
- SKC does not work across controllers in a mobility group.
- SKC works only on WPA2-enabled WLANs.
- SKC works only on local mode APs.

The following example shows how to enable Sticky PMKID Caching on WLAN 5:

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

config wlan security wpa wpa2 ciphers

To configure WPA2 ciphers and enable or disable Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) data encryption for WPA2, use the **config wlan security wpa wpa2 ciphers** command

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

Syntax Description

(Cisco Controller) > **aes**	Configures AES data encryption for WPA2.
tkip	Configures TKIP data encryption for WPA2.
enable	Enables AES or TKIP data encryption for WPA2.
disable	Disables AES or TKIP data encryption for WPA2.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

AES is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable AES data encryption for WPA2:

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

config wlan session-timeout

To change the timeout of wireless LAN clients, use the **config wlan session-timeout** command.

config wlan session-timeout {*wlan_id* | **foreignAp**} *seconds*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.
foreignAp	Specifies third-party access points.
seconds	Timeout or session duration in seconds. A value of zero is equivalent to no timeout. **Note** The range of session timeout depends on the security type: • Open system: 0-65535 (sec) • 802.1x: 300-86400 (sec) • static wep: 0-65535 (sec) • cranite: 0-65535 (sec) • fortress: 0-65535 (sec) • CKIP: 0-65535 (sec) • open+web auth: 0-65535 (sec) • web pass-thru: 0-65535 (sec) • wpa-psk: 0-65535 (sec) • disable: To disable reauth/session-timeout timers.

Command Default

None

Usage Guidelines

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the client timeout to 6000 seconds for WLAN ID 1:

```
(Cisco Controller) >config wlan session-timeout 1 6000
```

config wlan sip-cac disassoc-client

To enable client disassociation in case of session initiation protocol (SIP) call admission control (CAC) failure, use the **config wlan sip-cac disassoc-client** command.

config wlan sip-cac disassoc-client {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables a client disassociation on a SIP CAC failure.
disable	Disables a client disassociation on a SIP CAC failure.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Client disassociation for SIP CAC is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable a client disassociation on a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac disassoc-client enable 1
```

config wlan sip-cac send-486busy

To configure sending session initiation protocol (SIP) 486 busy message if a SIP call admission control (CAC) failure occurs, use the **config wlan sip-cac send-486busy** command:

config wlan sip-cac send-486busy {**enable** | **disable**} *wlan_id*

Syntax Description

enable	Enables sending a SIP 486 busy message upon a SIP CAC failure.
disable	Disables sending a SIP 486 busy message upon a SIP CAC failure.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

Session initiation protocol is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable sending a SIP 486 busy message upon a SIP CAC failure where the WLAN ID is 1:

```
(Cisco Controller) >config wlan sip-cac send-busy486 enable 1
```

config wlan static-ip tunneling

To configure static IP client tunneling support on a WLAN, use the **config wlan static-ip tunneling** command.

config wlan static-ip tunneling {**enable** | **disable**} *wlan_id*

Syntax Description

tunneling	Configures static IP client tunneling support on a WLAN.
enable	Enables static IP client tunneling support on a WLAN.
disable	Disables static IP client tunneling support on a WLAN.
wlan_id	Wireless LAN identifier from 1 to 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable static IP client tunneling support for WLAN ID 3:

```
(Cisco Controller) >config wlan static-ip tunneling enable 34
```

config wlan uapsd compliant client enable

To enable WPA1, use the **config wlan uapsd compliant-client enable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client enable*wlan-id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

Property Type	Property Value	Property Description

config wlan uapsd compliant-client disable

To disable WPA1, use the **config wlan uapsd compliant-client disable** command.

Note This was introduced for Ascom non-wmm capable phones and is not applicable for Cisco 792x/9971 IP phones.

config wlan uapsd compliant-client disable*wlan-id*

Syntax Description

wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable WPA1:

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

config wlan url-acl

To configure the WLAN's URL ACL, use the **config wlan url-acl** command.

config wlan url-acl*WLAN-id acl-name*

Syntax Description

WLAN-id	WLAN Identifier. The range is between 1 and 512
acl-name	Name of the ACL.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows how to cofigure a WLAN URL ACL:

```
(Cisco Controller) >config wlan url-acl 3 testacl
```

config wlan user-idle-threshold

To configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN, use the **config wlan user-idle-threshold** command.

config wlan user-idle-threshold *bytes wlan_id*

Syntax Description

bytes	Threshold data sent by the client during the idle timeout for the client session for a WLAN. If the client send traffic less than the defined threshold, the client is removed on timeout. The range is from 0 to 10000000 bytes.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default timeout for threshold data sent by client during the idle timeout is 0 bytes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the threshold data sent by the client during the idle timeout for client sessions for a WLAN:

```
(Cisco Controller) >config wlan user-idle-threshold 100 1
```

config wlan usertimeout

To configure the timeout for idle client sessions for a WLAN, use the **config wlan usertimeout** command.

config wlan usertimeout *timeout wlan_id*

Syntax Description

timeout	Timeout for idle client sessions for a WLAN. If the client sends traffic less than the threshold, the client is removed on timeout. The range is from 15 to 100000 seconds.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

The default client session idle timeout is 300 seconds.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The timeout value that you configure here overrides the global timeout that you define using the command **config network usertimeout**.

The following example shows how to configure the idle client sessions for a WLAN:

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan webauth-exclude

To release the guest user IP address when the web authentication policy time expires and exclude the guest user from acquiring an IP address for three minutes, use the **config wlan webauth-exclude** command.

config wlan webauth-exclude *wlan_id* {**enable** | **disable**}

Syntax Description

wlan_id	Wireless LAN identifier (1 to 512).
enable	Enables web authentication exclusion.
disable	Disables web authentication exclusion.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can use this command for guest WLANs that are configured with web authentication.

This command is applicable when you configure the internal DHCP scope on the controller.

By default, when the web authentication timer expires for a guest user, the guest user can immediately reassociate with the same IP address before another guest user can acquire the IP address. If there are many guest users or limited IP address in the DHCP pool, some guest users might not be able to acquire an IP address.

When you enable this feature on the guest WLAN, the guest user's IP address is released when the web authentication policy time expires and the guest user is excluded from acquiring an IP address for three minutes. The IP address is available for another guest user to use. After three minutes, the excluded guest user can reassociate and acquire an IP address, if available.

The following example shows how to enable the web authentication exclusion for WLAN ID 5:

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

config wlan wgb broadcast-tagging

To configure WGB broadcast tagging on a WLAN, use the **config wlan wgb broadcast-tagging** command.

config wlan wgb broadcast-tagging {**enable** | **disable**} *wlan-id*

Syntax Description

enable	Enables downlink broadcast packet VLAN tagging on a WLAN.
disable	Disables downlink broadcast packet VLAN tagging on a WLAN.
wlan-id	WLAN ID on which the configuration is to be applied.

Command Default

WGB broadcast tagging is disabled by default.

Command History

Release	Modification
8.3	This command was introduced.

The following example shows how to enable WGB broadcast tagging on WLAN ID 1:

```
(Cisco Controller) >config wlan wgb broadcast-tagging wlan 1
```

config wlan wifidirect

To configure Wi-Fi Direct Client Policy on a WLAN, use the **config wlan wifidirect** command.

config wlan wifidirect {**allow** | **disable** | **not-allow** | **xconnect-not-allow**} *wlan_id*

Syntax Description

allow	Allows Wi-Fi Direct clients to associate with the WLAN
disable	Ignores the Wi-Fi Direct status of clients thereby allowing Wi-Fi Direct clients to associate
not-allow	
xconnect-not-allow	Disallows the Wi-Fi Direct clients from associating with the WLAN
wlan_id	Wireless LAN identifier (1 to 16).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to allow Wi-Fi Direct Client Policy on WLAN ID 1:

```
(Cisco Controller) >config wlan wifidirect allow 1
```

config wlan wmm

To configure Wi-Fi Multimedia (WMM) mode on a wireless LAN, use the **config wlan wmm** command.

config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

Syntax Description

allow	Allows WMM on the wireless LAN.
disable	Disables WMM on the wireless LAN.
require	Specifies that clients use WMM on the specified wireless LAN.
wlan_id	Wireless LAN identifier (1 to 512).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When the controller is in Layer 2 mode and WMM is enabled, you must put the access points on a trunk port in order to allow them to join the controller.

The following example shows how to configure wireless LAN ID 1 to allow WMM:

```
(Cisco Controller) >config wlan wmm allow 1
```

The following example shows how to configure wireless LAN ID 1 to specify that clients use WMM:

```
(Cisco Controller) >config wlan wmm require 1
```

config wps ap-authentication

To configure access point neighbor authentication, use the **config wps ap-authentication** command.

config wps ap-authentication [**enable** | **disable threshold** *threshold_value*]

Syntax Description

enable	(Optional) Enables WMM on the wireless LAN.
disable	(Optional) Disables WMM on the wireless LAN.
threshold	(Optional) Specifies that WMM-enabled clients are on the wireless LAN.
threshold_value	Threshold value (1 to 255).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the access point neighbor authentication:

```
(Cisco Controller) > config wps ap-authentication threshold 25
```

Related Commands

show wps ap-authentication summary

config wps auto-immune

To enable or disable protection from Denial of Service (DoS) attacks, use the **config wps auto-immune** command.

config wps auto-immune {**enable** | **disable** | **stop**}

Syntax Description

enable	Enables the auto-immune feature.
disable	Disables the auto-immune feature.
stop	Stops dynamic auto-immune feature.

Command Default

Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A potential attacker can use specially crafted packets to mislead the Intrusion Detection System (IDS) into treating a legitimate client as an attacker. It causes the controller to disconnect this legitimate client and launch a DoS attack. The auto-immune feature, when enabled, is designed to protect against such attacks. However, conversations using Cisco 792x phones might be interrupted intermittently when the auto-immune feature is enabled. If you experience frequent disruptions when using 792x phones, you might want to disable this feature.

The following example shows how to configure the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune enable
```

The following example shows how to stop the auto-immune mode:

```
(Cisco Controller) > config wps auto-immune stop
Dynamic Auto Immune by WIPS is stopped
```

Related Commands

show wps summary

config wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the **config wps cids-sensor** command.

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*] }

Syntax Description

add	(Optional) Configures a new IDS sensor.
index	IDS sensor internal index.
ip_address	IDS sensor IP address.
username	IDS sensor username.
password	IDS sensor password.
delete	(Optional) Deletes an IDS sensor.
enable	(Optional) Enables an IDS sensor.
disable	(Optional) Disables an IDS sensor.
port	(Optional) Configures the IDS sensor's port number.
port	Port number.
interval	(Optional) Specifies the IDS sensor's query interval.
query_interval	Query interval setting.
fingerprint	(Optional) Specifies the IDS sensor's TLS fingerprint.
sha1	(Optional) Specifies the TLS fingerprint.
fingerprint	TLS fingerprint.

Command Default

Command defaults are listed below as follows:

Port	443
Query interval	60
Certification fingerprint	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
Query state	Disabled

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the intrusion detection system with the IDS index 1, IDS sensor IP address 10.0.0.51, IDS username Sensor_user0doc1, and IDS password passowrd01:

```
(Cisco Controller) > config wps cids-sensor add 1 10.0.0.51 Sensor_user0doc1 password01
```

Related Commands

show wps cids-sensor detail

config wps client-exclusion

To configure client exclusion policies, use the **config wps client-exclusion** command.

config wps client-exclusion {**802.11-assoc** | **802.11-auth** | **802.11x-auth** | **ip-theft** | **web-auth** | **all**} {**enable** | **disable**}

Syntax Description

802.11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
802.11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
802.1x-auth	Specifies that the controller excludes clients on the sixth 802.11X authentication attempt, after five consecutive failures.
ip-theft	Specifies that the control excludes clients if the IP address is already assigned to another device.
web-auth	Specifies that the controller excludes clients on the fourth web authentication attempt, after three consecutive failures.
all	Specifies that the controller excludes clients for all of the above reasons.
enable	Enables client exclusion policies.
disable	Disables client exclusion policies.

Command Default

All policies are enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable clients on the 802.11 association attempt after five consecutive failures:

```
(Cisco Controller) > config wps client-exclusion 802.11-assoc disable
```

Related Commands

show wps summary

config wps mfp

To configure Management Frame Protection (MFP), use the **config wps mfp** command.

config wps mfp {**infrastructure** | **ap-impersonation**} {**enable** | **disable**}

Syntax Description

infrastructure	Configures the MFP infrastructure.
ap-impersonation	Configures ap impersonation detection by MFP.
enable	Enables the MFP feature.
disable	Disables the MFP feature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the infrastructure MFP:

```
(Cisco Controller) > config wps mfp infrastructure enable
```

Related Commands

show wps mfp

config wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **config wps shun-list re-sync** command.

config wps shun-list re-sync

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the controller to synchronize with other controllers for the shun list:

```
(Cisco Controller) > config wps shun-list re-sync
```

Related Commands

show wps shun-list

config wps signature

To enable or disable Intrusion Detection System (IDS) signature processing, or to enable or disable a specific IDS signature, use the **config wps signature** command.

config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

Syntax Description

standard	Configures a standard IDS signature.
custom	Configures a standard IDS signature.
state	Specifies the state of the IDS signature.
signature_id	Identifier for the signature to be enabled or disabled.
enable	Enables the IDS signature processing or a specific IDS signature.
disable	Disables IDS signature processing or a specific IDS signature.

Command Default

IDS signature processing is enabled by default.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to enable IDS signature processing, which enables the processing of all IDS signatures:

```
(Cisco Controller) >config wps signature enable
```

The following example shows how to disable a standard individual IDS signature:

```
(Cisco Controller) > config wps signature standard state 15 disable
```

Related Commands

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

To specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected, use the **config wps signature frequency** command.

config wps signature frequency *signature_id frequency*

Syntax Description

signature_id	Identifier for the signature to be configured.
frequency	Number of matching packets per interval that must be at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval.

Command Default

The *frequency* default value varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per access point before an attack is detected to 1800 for signature ID 4:

```
(Cisco Controller) > config wps signature frequency 4 1800
```

Related Commands

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

To specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval, use the **config wps signature interval** command.

config wps signature interval *signature_id interval*

Syntax Description

signature_id	Identifier for the signature to be configured.
interval	Number of seconds that must elapse before the signature frequency threshold is reached. The range is 1 to 3,600 seconds.

Command Default

The default value of *interval* varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds to elapse before reaching the signature frequency threshold to 200 for signature ID 1:

```
(Cisco Controller) > config wps signature interval 1 200
```

Related Commands

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

To specify the number of matching packets per interval that must be identified per client per access point before an attack is detected, use the **config wps signature mac-frequency** command.

config wps signature mac-frequency *signature_id mac_frequency*

Syntax Description

signature_id	Identifier for the signature to be configured.
mac_frequency	Number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval.

Command Default

The *mac_frequency* default value varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of matching packets per interval per client before an attack is detected to 50 for signature ID 3:

```
(Cisco Controller) > config wps signature mac-frequency 3 50
```

Related Commands

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

To specify the length of time after which no attacks have been detected at the individual access point level and the alarm can stop, use the **config wps signature quiet-time** command.

config wps signature quiet-time *signature_id quiet_time*

Syntax Description

signature_id	Identifier for the signature to be configured.
quiet_time	Length of time after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds.

Command Default

The default value of *quiet_time* varies per signature.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to set the number of seconds after which no attacks have been detected per access point to 60 for signature ID 1:

```
(Cisco Controller) > config wps signature quiet-time 1 60
```

Related Commands

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

To reset a specific Intrusion Detection System (IDS) signature or all IDS signatures to default values, use the **config wps signature reset** command.

config wps signature reset {*signature_id* | **all**}

Syntax Description

signature_id	Identifier for the specific IDS signature to be reset.
all	Resets all IDS signatures.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

The following example shows how to reset the IDS signature 1 to default values:

```
(Cisco Controller) > config wps signature reset 1
```

Related Commands

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

PART IV

Debug Commands

- Debug Commands: 802.11, on page 1233
- Debug Commands: a to i, on page 1241
- Debug Commands: j to q, on page 1311
- Debug Commands: r to z, on page 1337

Debug Commands: 802.11

- debug 11k, on page 1234
- debug 11w-pmf, on page 1235
- debug 11v all, on page 1236
- debug 11v detail, on page 1237
- debug 11v error, on page 1238
- debug 11w-pmf, on page 1239

debug 11k

To configure the debugging of 802.11k settings, use the **debug 11k** command.

debug 11k { **all** | **detail** | **errors** | **events** | **history** | **optimization** | **simulation** } { **enable** | **disable** }

Syntax Description

all	Configures the debugging of all 802.11k messages.
detail	Configures the debugging of 802.11k details.
errors	Configures the debugging of 802.11k errors.
events	Configures the debugging of all 802.11k events.
history	Configures the debugging of all 802.11k history. The controller collects roam history of the client.
optimization	Configures the debugging of 802.11k optimizations. You can view optimization steps of neighbor lists.
simulation	Configures the debugging of 802.11k simulation data. You can view details of client roaming parameters and import them for offline simulation.
enable	Enables the 802.1k debugging.
disable	Disables the 802.1k debugging.

Command Default

None.

This example shows how to enable the debugging of 802.11k simulation data:

```
(Cisco Controller) >debug 11k simulation enable
```

Related Commands

config assisted-roaming

config wlan assisted-roaming

show assisted-roaming

debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11w messages.
keys	Configures the debugging of 802.11w keys.
events	Configures the debugging of 802.11w events.
enable	Enables the debugging of 802.1w options.
disable	Disables the debugging of 802.1w options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

debug 11v all

To configure the 802.11v debug options, use the **debug 11v all** command.

debug 11v all {**enable | disable**}

Syntax Description

enable	Enables all the debug.
disable	Disables all the debug.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable all the debug:

```
(Cisco Controller) >debug 11v all enable
```

debug 11v detail

To configure the 802.11v debug details, use the **debug 11v detail** command.

debug 11v detail {**enable | disable**}

Syntax Description

enable	Enables debug details.
disable	Disables debug details.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable 802.11v debug details:

```
(Cisco Controller) >debug 11v detail enable
```

debug 11v error

To configure the 802.11v error debug options, use the **debug 11v errors** command.

debug 11v errors {**enable** | **disable**}

Syntax Description

enable	Enables error debug.
disable	Disables error debug.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable 802.11v error debug:

```
(Cisco Controller) >debug 11v error enable
```

debug 11w-pmf

To configure the debugging of 802.11w, use the **debug 11w-pmf** command.

debug 11w-pmf {**all** | **events** | **keys**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11w messages.
keys	Configures the debugging of 802.11w keys.
events	Configures the debugging of 802.11w events.
enable	Enables the debugging of 802.1w options.
disable	Disables the debugging of 802.1w options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11w keys:

```
(Cisco Controller) >debug 11w-pmf keys enable
```

Debug Commands: a to i

- debug aaa, on page 1243
- debug aaa events, on page 1244
- debug aaa local-auth, on page 1245
- debug airewave-director, on page 1247
- debug ap, on page 1249
- debug ap enable, on page 1251
- debug ap packet-dump, on page 1252
- debug ap show stats, on page 1253
- debug ap show stats video, on page 1255
- debug arp, on page 1256
- debug avc, on page 1257
- debug bcast, on page 1258
- debug call-control, on page 1259
- debug capwap, on page 1260
- debug capwap reap, on page 1261
- debug ccxdiag, on page 1262
- debug ccxrm, on page 1263
- debug ccxs69, on page 1264
- debug cckm, on page 1265
- debug client, on page 1266
- debug cts aaa, on page 1267
- debug cts authz, on page 1268
- debug cts capwap, on page 1269
- debug cts env-data, on page 1270
- debug cts ha, on page 1271
- debug cts key-store, on page 1272
- debug cts provisioning, on page 1273
- debug cts sgt, on page 1274
- debug cts sxp, on page 1275
- debug cac, on page 1276
- debug cdp, on page 1277
- debug crypto, on page 1278
- debug dhcp, on page 1279

- debug dhcp service-port, on page 1280
- debug disable-all, on page 1281
- debug dns, on page 1282
- debug dot11, on page 1283
- debug dot11, on page 1284
- debug dot11 mgmt interface, on page 1285
- debug dot11 mgmt msg, on page 1286
- debug dot11 mgmt ssid, on page 1287
- debug dot11 mgmt state-machine, on page 1288
- debug dot11 mgmt station, on page 1289
- debug dot1x, on page 1290
- debug dtls, on page 1291
- debug fastpath , on page 1292
- debug flexconnect avc, on page 1297
- debug flexconnect aaa, on page 1298
- debug flexconnect acl, on page 1299
- debug flexconnect cckm, on page 1300
- debug group, on page 1301
- debug fmchs, on page 1302
- debug flexconnect client ap, on page 1303
- debug flexconnect client ap syslog, on page 1304
- debug flexconnect client group, on page 1305
- debug flexconnect client group syslog, on page 1306
- debug flexconnect group, on page 1307
- debug ft, on page 1308
- debug hotspot, on page 1309
- debug ipv6, on page 1310

debug aaa

To configure the debugging of AAA settings, use the **debug aaa** command.

debug aaa {[**all** | **avp-xml** | **detail** | **events** | **packet** | **ldap** | **local-auth** | **tacacs**] [**enable** | **disable**]}

Syntax Description

all	(Optional) Configures the debugging of all AAA messages.
avp-xml	(Optional) Configures debug of AAA Avp xml events.
detail	(Optional) Configures the debugging of AAA errors.
events	(Optional) Configures the debugging of AAA events.
packet	(Optional) Configures the debugging of AAA packets.
ldap	(Optional) Configures the debugging of the AAA Lightweight Directory Access Protocol (LDAP) events.
local-auth	(Optional) Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) events.
tacacs	(Optional) Configures the debugging of the AAA TACACS+ events.
enable	(Optional) Enables the debugging.
disable	(Optional) Disables the debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of AAA LDAP events:

```
(Cisco Controller) > debug aaa ldap enable
```

Related Commands

debug aaa local-auth eap

show running-config

debug aaa events

To configure the debugging related to DNS-based ACLs, use the **debug aaa events enable** command.

debug aaa events enable

Syntax Description

events	Configures the debugging of DNS-based ACLs.

Command History

Release	Modification
7.6	This command is introduced.

The following example shows how to enable the debugging for DNS-based ACLs:

```
(Cisco Controller) > debug aaa events enble
```

debug aaa local-auth

To configure the debugging of AAA local authentication on the controller, use the **debug aaa local-auth** command.

debug aaa local-auth { **db** | **shim** | **eap** { **framework** | **method** } { **all** | **errors** | **events** | **packets** | **sm** } } { **enable** | **disable** }

Syntax Description

db	Configures the debugging of the AAA local authentication back-end messages and events.
shim	Configures the debugging of the AAA local authentication shim layer events.
eap	Configures the debugging of the AAA local Extensible Authentication Protocol (EAP) authentication.
framework	Configures the debugging of the local EAP framework.
method	Configures the debugging of local EAP methods.
all	Configures the debugging of local EAP messages.
errors	Configures the debugging of local EAP errors.
events	Configures the debugging of local EAP events.
packets	Configures the debugging of local EAP packets.
sm	Configures the debugging of the local EAP state machine.
enable	Starts the debugging.
disable	Stops the debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the AAA local EAP authentication:

```
(Cisco Controller) > debug aaa local-auth eap method all enable
```

Related Commands

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

To configure the debugging of Airewave Director software, use the **debug airwave-director** command.

debug airewave-director {**all** | **channel** | **detail** | **error** | **group** | **manager** | **message** | **packet** | **power** | **profile** | **radar** | **rf-change**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all Airewave Director logs.
channel	Configures the debugging of the Airewave Director channel assignment protocol.
detail	Configures the debugging of the Airewave Director detail logs.
error	Configures the debugging of the Airewave Director error logs.
group	Configures the debugging of the Airewave Director grouping protocol.
manager	Configures the debugging of the Airewave Director manager.
message	Configures the debugging of the Airewave Director messages.
packet	Configures the debugging of the Airewave Director packets.
power	Configures the debugging of the Airewave Director power assignment protocol and coverage hole detection.
profile	Configures the debugging of the Airewave Director profile events.
radar	Configures the debugging of the Airewave Director radar detection/avoidance protocol.
rf-change	Configures the debugging of the Airewave Director rf changes.
enable	Enables the Airewave Director debugging.
disable	Disables the Airewave Director debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of Airewave Director profile events:

```
(Cisco Controller) > debug airewave-director profile enable
```

Related Commands

debug disable-all

show sysinfo

debug ap

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables the debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables the debugging on a lightweight access point. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

The remote debugging of Cisco lightweight access points is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to execute the **config ap location** command on access point AP02:

```
(Cisco Controller) >debug ap command "config ap location "Building 1" AP02"
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap enable

To configure the remote debugging of Cisco lightweight access points or to remotely execute a command on a lightweight access point, use the **debug ap enable** command.

debug ap {**enable** | **disable** | **command** *cmd*} *cisco_ap*

Syntax Description

enable	Enables the remote debugging. **Note** The debugging information is displayed only to the controller console and does not send output to a controller Telnet/SSH CLI session.
disable	Disables the remote debugging.
command	Specifies that a CLI command is to be executed on the access point.
cmd	Command to be executed. **Note** The command to be executed must be enclosed in double quotes, such as **debug ap command "led flash 30" AP03**. The output of the command displays only to the controller console and does not send output to a controller Telnet/SSH CLI session.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the remote debugging on access point AP01:

```
(Cisco Controller) >debug ap enable AP01
```

The following example shows how to disable the remote debugging on access point AP02:

```
(Cisco Controller) >debug ap disable AP02
```

The following example shows how to execute the flash LED command on access point AP03:

```
(Cisco Controller) >debug ap command "led flash 30" AP03
```

debug ap packet-dump

To configure the debugging of Packet Capture, use the **debug ap packet-dump** command.

debug ap packet-dump { **enable** | **disable** }

Syntax Description

enable	Enables the debugging of Packet Capture of an access point.
disable	Disables the debugging of Packet Capture of an access point.

Command Default

Debugging of Packet Capture is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Packet Capture does not work during inter-controller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as beacon or probe response. Only packets that flow through the radio driver in the Tx path will be captured.

The following example shows how to enable the debugging of Packet Capture from an access point:

```
(Cisco Controller) >debug ap packet-dump enable
```

debug ap show stats

To debug video messages and statistics of Cisco lightweight access points, use the **debug ap show stats** command.

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**}

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.
tx-queue	Displays the transmit queue traffic statistics of the AP.
packet	Displays the packet statistics of the AP.
load	Displays the QoS Basic Service Set (QBSS) and other statistics of the AP.
multicast	Displays the multicast supported rate statistics of the AP.
client	Displays the specified client metric statistics.
client_MAC	MAC address of the client.
video	Displays video statistics of all clients on the AP.
all	Displays statistics of all clients on the AP.
video metrics	Displays the video metric statistics.
mgid	Displays detailed multicast information for a single multicast group ID (MGID).
mgid_database_number	Layer 2 MGID database number.
admission	Displays video admission control on the AP.
bandwidth	Displays video bandwidth on the AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to troubleshoot the access point AP01's transmit queue traffic on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 tx-queue
```

The following example shows how to troubleshoot the access point AP02's multicast supported rates on an 802.11b/g network:

```
(Cisco Controller) >debug ap show stats 802.11b AP02 multicast
```

The following example shows how to troubleshoot the metrics of a client identified by its MAC address, associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client 00:40:96:a8:f7:98
```

The following example shows how to troubleshoot the metrics of all clients associated with the access point AP01 on an 802.11a network:

```
(Cisco Controller) >debug ap show stats 802.11a AP01 client all
```

debug ap show stats video

To configure the debugging of video messages and statistics of Cisco lightweight access points, use the **debug ap show stats video** command.

debug ap show stats video *cisco_ap* {**multicast mgid** *mgid_value* | **admission** | **bandwidth**}

Syntax Description

cisco_ap	Cisco lightweight access point name.
multicast mgid	Displays multicast database related information for the specified MGID of an access point.
mgid_value	Layer 2 MGID database number from 1 to 4095.
admission	Displays the video admission control.
bandwidth	Displays the video bandwidth.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of an access point AP01's multicast group that is identified by the group's Layer 2 MGID database number:

```
(Cisco Controller) >debug ap show stats video AP01 multicast mgid 50
```

This example shows how to configure the debugging of an access point AP01's video bandwidth:

```
(Cisco Controller) >debug ap show stats video AP01 bandwidth
```

debug arp

To configure the debugging of Address Resolution Protocol (ARP) options, use the **debug arp** command.

debug arp {**all** | **detail** | **events** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all ARP logs.
detail	Configures the debugging of ARP detail messages.
error	Configures the debugging of ARP errors.
message	Configures the debugging of ARP messages.
enable	Enables the ARP debugging.
disable	Disables the ARP debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable ARP debug settings:

```
(Cisco Controller) > debug arp error enable
```

The following example shows how to disable ARP debug settings:

```
(Cisco Controller) > debug arp error disable
```

Related Commands

debug disable-all

show sysinfo

debug avc

To configure the debugging of Application Visibility and Control (AVC) options, use the **debug avc error** command.

debug avc {**events** | **error**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of AVC events.
error	Configures the debugging of AVC errors.
enable	Enables the debugging of AVC events or errors.
disable	Disables the debugging of AVC events or errors.

Command Default

By default, the debugging of AVC options is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of AVC errors:

```
(Cisco Controller) > debug avc error enable
```

Related Commands

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug bcast

To configure the debugging of broadcast options, use the **debug bcast** command.

debug bcast {**all** | **error** | **message** | **igmp** | **detail**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all broadcast logs.
error	Configures the debugging of broadcast errors.
message	Configures the debugging of broadcast messages.
igmp	Configures the debugging of broadcast IGMP messages.
detail	Configures the debugging of broadcast detailed messages.
enable	Enables the broadcast debugging.
disable	Disables the broadcast debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of broadcast messages:

```
(Cisco Controller) > debug bcast message enable
```

The following example shows how to disable the debugging of broadcast mesages:

```
(Cisco Controller) > debug bcast message disable
```

Related Commands

debug disable-all

show sysinfo

debug call-control

To configure the debugging of the SIP call control settings, use the **debug call-control** command.

debug call-control {**all** | **event**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging options for all SIP call control messages.
event	Configures the debugging options for SIP call control events.
enable	Enables the debugging of SIP call control messages or events.
disable	Disables the debugging of SIP call control messages or events.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of all SIP call control messages:

```
(Cisco Controller) >debug call-control all enable
```

debug capwap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings, use the **debug capwap** command.

debug capwap {**detail** | **dtls-keepalive** | **errors** | **events** | **hexdump** | **info** | **packet** | **payload** | **mfp**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging for CAPWAP detail settings.
dtls-keepalive	Configures the debugging for CAPWAP DTLS data keepalive packets settings.
errors	Configures the debugging for CAPWAP error settings.
events	Configures the debugging for CAPWAP events settings.
hexdump	Configures the debugging for CAPWAP hexadecimal dump settings.
info	Configures the debugging for CAPWAP info settings.
packet	Configures the debugging for CAPWAP packet settings.
payload	Configures the debugging for CAPWAP payload settings.
mfp	Configures the debugging for CAPWAP mfp settings.
enable	Enables the debugging of the CAPWAP command.
disable	Disables the debugging of the CAPWAP command.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of CAPWAP details:

```
(Cisco Controller) >debug capwap detail enable
```

debug capwap reap

To configure the debugging of Control and Provisioning of Wireless Access Points (CAPWAP) settings on a FlexConnect access point, use the **debug capwap reap** command.

debug capwap reap [**mgmt** | **load**]

Syntax Description

mgmt	(Optional) Configures the debugging for client authentication and association messages.
load	(Optional) Configures the debugging for payload activities, which is useful when the FlexConnect access point boots up in standalone mode.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of FlexConnect client authentication and association messages:

```
(Cisco Controller) >debug capwap reap mgmt
```

debug ccxdiag

To configure debugging of Cisco Compatible Extensions (CCX) diagnostic options, use the **debug ccxdiag** command.

debug ccxdiag {**all** | **error** | **event** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CCX S69 messages.
error	Configures debugging of the CCX S69 errors.
event	Configures debugging of the CCX S69 events.
packet	Configures debugging of the CCX S69 packets.
enable	Enables debugging of the CCX S69 options.
disable	Disables debugging of the CCX S69 options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX S69 packets debugging:

```
(Cisco Controller) >debug ccxdiag packets enable
```

debug ccxrm

To configure debugging of the CCX Cisco Client eXtension (CCX) Radio Management (RM), use the **debug ccxrm** command.

debug ccxrm {**all** | **detail** | **error** | **location-calibration** | **message** | **packet** | **warning**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all CCX RM messages.
detail	Configures detailed debugging of CCX RM.
error	Configures debugging of the CCX RM errors.
location-calibration	Configures debugging of the CCX RM location calibration.
message	Configures debugging of CCX RM messages.
packet	Configures debugging of the CCX RM packets.
warning	Configures debugging of the CCX RM warnings.
enable	Enables debugging of the CCX RM options.
disable	Disables debugging of the CCX RM options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX RM debugging:

```
(Cisco Controller) > debug ccxrm all enable
```

debug ccxs69

To configure debugging of CCX S69 tasks, use the **debug ccxs69** command.

debug ccxs69 {**all** | **error** | **event**} {**enable**| **disable**}

Syntax Description

all	Configures debugging of all the CCX S69 messages.
error	Configures debugging of the CCX S69 errors.
event	Configures debugging of the CCX S69 events.
enable	Enables debugging of the CCX S69 options.
disable	Disables debugging of the CCX S69 options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CCX S69 debugging:

```
(Cisco Controller) >debug ccxs69 all enable
```

debug cckm

To configure the debugging of the Cisco Centralized Key Management options, use the **debug cckm**

debug cckm {**client** | **detailed**} {**enable** | **disable**}

Syntax Description

client	Configures debugging of the Cisco Centralized Key Management of clients.
detailed	Configures detailed debugging of Cisco Centralized Key Management.
enable	Enables debugging of Cisco Centralized Key Management.
disable	Disables debugging of Cisco Centralized Key Management.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable detailed debugging of Cisco Centralized Key Management:

```
(Cisco Controller) > debug cckm detailed enable
```

debug client

To configure the debugging for a specific client, use the **debug client** command.

debug client *mac_address*

Syntax Description

mac_address	MAC address of the client.

Command Default

None

Usage Guidelines

After entering the **debug client** *mac_address* command, if you enter the **debug aaa events enable** command, then the AAA events logs are displayed for that particular client MAC address.

Command History

Release	Modification
7.6	This command was introduced.

The following example shows how to debug a specific client:

```
(Cisco Controller) > debug client 01:35:6x:yy:21:00
```

debug cts aaa

To configure the Cisco TrustSec AAA debug options, use the **debug cts aaa** command.

debug cts aaa {**all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CTS AAA debug options
errors	Configures debugging of all the CTS AAA errors
events	Configures debugging of all the CTS AAA events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts authz

To configure the Cisco TrustSec security group access control list (SGACL) download debug options, use the **debug cts authz** command.

debug cts authz {**aaa** | **all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

aaa	Configures debugging of CTS AAA policy
all	Configures debugging of all the CTS policies
errors	Configures debugging of all the CTS policy errors
events	Configures debugging of all the CTS policy events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts capwap

To configure the debug options for Cisco TrustSec policy download over CAPWAP messages, use the **debug cts capwap** command.

debug cts capwap {**messages** | **all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

messages	Configures debugging of Protected Access Credential (PAC) CAPWAP messages
all	Configures debugging of all the CTS CAPWAP messages
errors	Configures debugging of the PAC CAPWAP errors
events	Configures debugging of the PAC CAPWAP events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts env-data

To configure Cisco TrustSec environment data debugs, use the **debug cts env-data** command.

debug cts env-data {**all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CTS environment data
errors	Configures debugging of CTS environment data errors
events	Configures debugging of CTS environment data events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts ha

To configure the Cisco TrustSec High Availability (HA) debug options, use the **debug cts ha** command.

debug cts ha {**all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CTS HA options
errors	Configures debugging of CTS HA errors
events	Configures debugging of CTS HA events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts key-store

To configure the Cisco TrustSec Key-store debug options, use the **debug cts key-store** command.

debug cts key-store {**enable** | **disable**}

Syntax Description

enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts provisioning

To configure the Cisco TrustSec PAC Provisioning debug options, use the **debug cts provisioning** command.

debug cts provisioning {**packets** | **all** | **errors** | **events**} {**enable** | **disable**}

Syntax Description

packets	Configures debugging of PAC provisioning packets
all	Configures debugging of all the PAC provisioning options
errors	Configures debugging of the PAC provisioning errors
events	Configures debugging of the PAC provisioning events
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts sgt

To configure debugging of up to 10 SGTs, use the **debug cts sgt** command.

debug cts sgt {*sgt-1* | *sgt-2* | *sgt-3* | *sgt-4* | *sgt-5* | *sgt-6* | *sgt-7* | *sgt-8* | *sgt-9* | *sgt-10*}

Syntax Description

sgt-1 to *sgt-10*	SGT IDs that you have to enter.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

debug cts sxp

To configure debugging of Cisco TrustSec SXP options, use the **debug cts sxp** command.

debug cts sxp {**all** | **errors** | **events** | **framework** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the CTS SXP options
errors	Configures debugging of the CTS SXP errors
events	Configures debugging of the CTS SXP events
framework	Configures debugging of the CTS SXP framework
message	Configures debugging of the CTS SXP messages
enable	Enables debugging
disable	Disables debugging

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

debug cac

To configure the debugging of Call Admission Control (CAC) options, use the **debug cac** command.

debug cac {**all** | **event** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging options for all CAC messages.
event	Configures the debugging options for CAC events.
packet	Configures the debugging options for selected CAC packets.
kts	Configures the debugging options for KTS-based CAC messages.
enable	Enables the debugging of CAC settings.
disable	Disables the debugging of CAC settings.

Command Default

By default, the debugging of CAC options is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of CAC settings:

```
(Cisco Controller) > debug cac event enable
(Cisco Controller) > debug cac packet enable
```

Related Commands

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

To configure debugging of CDP, use the **debug cdp** command.

debug cdp {**events** | **packets**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of the CDP events.
packets	Configures debugging of the CDP packets.
enable	Enables debugging of the CDP options.
disable	Disables debugging of the CDP options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable CDP event debugging in a Cisco controller:

```
(Cisco Controller) > debug cdp
```

debug crypto

To configure the debugging of the hardware cryptographic options, use the **debug crypto** command.

debug crypto {**all** | **sessions** | **trace** | **warning**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all hardware crypto messages.
sessions	Configures the debugging of hardware crypto sessions.
trace	Configures the debugging of hardware crypto sessions.
warning	Configures the debugging of hardware crypto sessions.
enable	Enables the debugging of hardware cryptographic sessions.
disable	Disables the debugging of hardware cryptographic sessions.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of hardware crypto sessions:

```
(Cisco Controller) > debug crypto sessions enable
```

Related Commands

debug disable-all

show sysinfo

debug dhcp

To configure the debugging of DHCP, use the **debug dhcp** command.

debug dhcp {**message** | **packet**} {**enable** | **disable**}

Syntax Description

message	Configures the debugging of DHCP error messages.
packet	Configures the debugging of DHCP packets.
enable	Enables the debugging DHCP messages or packets.
disable	Disables the debugging of DHCP messages or packets.

Command Default

None

The following example shows how to enable the debugging of DHCP messages:

```
(Cisco Controller) >debug dhcp message enable
```

debug dhcp service-port

To enable or disable debugging of the Dynamic Host Configuration Protocol (DHCP) packets on the service port, use the **debug dhcp service-port** command.

debug dhcp service-port {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of DHCP packets on the service port.
disable	Disables the debugging of DHCP packets on the service port.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of DHCP packets on a service port:

```
(Cisco Controller) >debug dhcp service-port enable
```

debug disable-all

To disable all debug messages, use the **debug disable-all** command.

debug disable-all

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to disable all debug messages:

```
(Cisco Controller) > debug disable-all
```

debug dns

To configure debugging of Domain Name System (DNS) options, use the **debug dns** command.

debug dns {**all** | **detail** | **error** | **message**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DNS options.
detail	Configures debugging of the DNS details.
error	Configures debugging of the DNS errors.
message	Configures debugging of the DNS messages.
enable	Enables debugging of the DNS options.
disable	Disables debugging of the DNS options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable DNS error debugging:

```
(Cisco Controller) > debug dns error enable
```

debug dot11

To configure the debugging of 802.11 events, use the **debug dot11** command.

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11 messages.
load-balancing	Configures the debugging of 802.11 load balancing events.
management	Configures the debugging of 802.11 MAC management messages.
mobile	Configures the debugging of 802.11 mobile events.
nmsp	Configures the debugging of the 802.11 NMSP interface events.
probe	Configures the debugging of probe.
rldp	Configures the debugging of 802.11 Rogue Location Discovery.
rogue	Configures the debugging of 802.11 rogue events.
state	Configures the debugging of 802.11 mobile state transitions.
enable	Enables the 802.11 debugging.
disable	Disables the 802.11 debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11 settings:

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

debug dot11

To configure the debugging of 802.11 events, use the **debug dot11** command.

debug dot11 {**all** | **load-balancing** | **management** | **mobile** | **nmsp** | **probe** | **rldp** | **rogue** | **state**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all 802.11 messages.
load-balancing	Configures the debugging of 802.11 load balancing events.
management	Configures the debugging of 802.11 MAC management messages.
mobile	Configures the debugging of 802.11 mobile events.
nmsp	Configures the debugging of the 802.11 NMSP interface events.
probe	Configures the debugging of probe.
rldp	Configures the debugging of 802.11 Rogue Location Discovery.
rogue	Configures the debugging of 802.11 rogue events.
state	Configures the debugging of 802.11 mobile state transitions.
enable	Enables the 802.11 debugging.
disable	Disables the 802.11 debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of 802.11 settings:

```
(Cisco Controller) > debug dot11 state enable
(Cisco Controller) > debug dot11 mobile enable
```

debug dot11 mgmt interface

To configure debugging of 802.11 management interface events, use the **debug dot11 mgmt interface** command.

debug dot11 mgmt interface

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to debug 802.11 management interface events:

```
(Cisco Controller) >debug dot11 mgmt interface
```

debug dot11 mgmt msg

To configure debugging of 802.11 management messages, use the **debug dot11 mgmt msg** command.

debug dot11 mgmt msg

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to debug dot11 management messages:

```
(Cisco Controller) >debug dot11 mgmt msg
```

debug dot11 mgmt ssid

To configure debugging of 802.11 SSID management events, use the **debug dot11 mgmt ssid** command.

debug dot11 mgmt ssid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of 802.11 SSID management events:

```
(Cisco Controller) >debug dot11 mgmt ssid
```

debug dot11 mgmt state-machine

To configure debugging of the 802.11 state machine, use the **debug dot11 mgmt state-machine** command.

debug dot11 mgmt state-machine

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of 802.11 state machine:

```
(Cisco Controller) >debug dot11 mgmt state-machine
```

debug dot11 mgmt station

To configure the debugging of the management station settings, use the **debug dot11 mgmt station** command.

debug dot11 mgmt station

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of the management station settings:

```
(Cisco Controller) >debug dot11 mgmt station
```

debug dot1x

To configure debugging of the 802.1X options, use the **debug dot1x** command.

debug dot1x {**aaa** | **all** | **events** | **packets** | **states**} {**enable** | **disable**}

Syntax Description

aaa	Configures debugging of the 802.1X AAA interactions.
all	Configures debugging of all the 802.1X messages.
events	Configures debugging of the 802.1X events.
packets	Configures debugging of the 802.1X packets.
states	Configures debugging of the 802.1X state transitions.
enable	Enables debugging of the 802.1X options.
disable	Disables debugging of the 802.1X options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable 802.1X state transitions debugging:

```
(Cisco Controller) > debug dot1x states enable
```

debug dtls

To configure debugging of the Datagram Transport Layer Security (DTLS) options, use the **debug dtls** command.

debug dtls {**all** | **event** | **packet** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the DTLS messages.
event	Configures debugging of the DTLS events.
packet	Configures debugging of the DTLS packets.
trace	Configures debugging of the DTLS trace messages.
enable	Enables debugging of the DTLS options.
disable	Disables debugging of the DTLS options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The debug actions described here are used in conjunction with CAPWAP troubleshooting.

The following example shows how to enable DTLS packet debugging:

```
(Cisco Controller) > debug dtls packet enable
```

debug fastpath

To debug the issues in the 10-Gigabit Ethernet interface of the controller and to view details of all the management and control features of the controller, use the **debug fastpath** command.

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**}]

Syntax Description

disable	Enables debug of fastpath messages.
enable	Disables debug of fastpath messages.
errors	Displays the debug messages related to the fastpath errors.
events	Displays the debug messages related to the fastpath events.
warnings	Displays the debug messages related to the fastpath warnings.
log	Configures debug of log messages.
errors	Configures debug of fastpath errors.
events	Configures debug of fastpath events.
show	Displays log of most recent events related to fastpath.
status	Displays status of fastpath configuration.
dump	Displays the CLI dump commands.
stats	Displays the debug statistics from the data plane.
DP_number	Displays the statistic counters at data plane based on selected data plane number. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.

fpapool	Displays statistics of packet buffer in data plane.
DP_number	Displays statistics of packet buffer based on data plane number. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
ownerdb	Displays the data plane owner information.
portdb	Displays the port database at data plane.
tun4db	Dumps the first 20 tunnels from the data plane.
index	Dumps 20 tunnel entries from index provided. You must use data plane number 0/1 to denote WISM2 data plane processor.
DP_number	Dumps the first twenty client entries from the data plane. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
scbdb	Dumps 20 client entries starting from index provided. You must use data plane number 0/1 to denote WISM2 data plane processor.
index	Dumps client information for the selected MAC address.

DP_number	Dumps the first twenty client entries from the data plane. Values include 0, 1, and All. The default option is All. You must select: • The index 0 for the Cisco Wireless LAN Controller 2504 Series, Cisco Wireless LAN Controller 5508 Series, Cisco Wireless LAN Controller 7500 Series, Cisco Wireless LAN Controller 8500 Series. • The index 0 and/or 1 respectively for the two data planes in WiSM2 to view statistics of individual data plane or from both.
cfgtool -- dump.sfp	Displays the model/type of SX/LC/T small form-factor plug-in (SFP) modules with the OUI Partnumber.
urlacldb *start-acl-id start-rule-index*	Dumps the URL ACL database.
vlandb	Dumps the VLAN database in the dataplane.
dpcp-stats	Displays the dataplane to controlplane message statistics.
clear stats	Clears the data plane statistic counters.
systemdb	Displays the global data plane configuration.
debug	Displays the few latest messages of the data plane to enable troubleshooting.
wlanappstats	Displays Application Visibility and Control (AVC) statistics of a WLAN.
wlan_id	The WLAN identifier of the WLAN you need identify the AVC statistics.
appqosdb	Displays Application Visibility and Control (AVC) database statistics of the data plane.
clear	Clear command.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.3	This command was enhanced in this release. The new keyword added is urlacldb

Usage Guidelines

None

Examples

The following is an example of the SX/LC/T small form-factor plug-in (SFP) modules model/type with the respective OUI Partnumber.

```
(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
```

The following is an example of the fastpath status displayed while you execute the status command.

```
 (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
```

The following is an example of the fastpath errors displayed while you execute the debug fastpath log errors command.

```
(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
```

The following is an example of the fastpath events displayed while you execute the debug fastpath log events command.

```
(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
```

The following is an example displayed while you execute the debug fastpath log show command.

```
(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

To debug a Flexconnect Application Visibility and Control (AVC) event, use the **debug flexconnect avc** command.

debug flexconnect ave {**event** | **error** | **detail**} {**enable** | **disable**}

Syntax Description

event	Debugsa FlexConnect AVC event.
error	Debugs a FlexConnect AVC error.
detail	Debugs a FlexConnect AVC details.
enable	Enables debug.
disable	Disables debug.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to enable a debug action for an event:

```
(Cisco Controller) >debug flexconnect avc event enable
```

debug flexconnect aaa

To configure debugging of FlexConnect backup RADIUS server events or errors, use the **debug flexconnect aaa** command.

debug flexconnect aaa {**event** | **error**} {**enable** | **disable**}

Syntax Description

event	Configures the debugging for FlexConnect RADIUS server events.
error	Configures the debugging for FlexConnect RADIUS server errors.
enable	Enables the debugging of FlexConnect RADIUS server settings.
disable	Disables the debugging of FlexConnect RADIUS server settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect RADIUS server events:

```
(Cisco Controller) >debug flexconnect aaa event enable
```

debug flexconnect acl

Configures debugging of FlexConnect access control lists (ACLs), use the **debug flexconnect acl** command.

debug flexconnect acl {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect ACLs.
disable	Disables the debugging of FlexConnect ACLs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect ACLs:

```
(Cisco Controller) >debug flexconnect acl enable
```

debug flexconnect cckm

Configure debugging of FlexConnect Cisco Centralized Key Management (CCKM) fast roaming, use the **debug flexconnect cckm** command.

debug flexconnect cckm {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect CCKM fast roaming settings.
disable	Disables the debugging of FlexConnect CCKM fast roaming settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect CCKM fast roaming events:

```
(Cisco Controller) >debug flexconnect cckm event enable
```

debug group

To configure the debugging of access point groups, use the **debug group** command.

debug group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of access point groups.
disable	Disables the debugging of access point groups.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of access point groups:

```
(Cisco Controller) >debug group enable
```

debug fmchs

To configure debugging of Fixed Mobile Convergence Handover Service (FMCHS) of the controller, use the **debug fmchs**command.

debug fmchs {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all FMCHS messages.
error	Configures debugging of the FMCHS errors.
event	Configures debugging of the FMCHS events.
nmsp	Configures debugging of the FMCHS NMSP events.
packet	Configures debugging of the FMCHS packets.
enable	Enables debugging of the FMCHS options.
disable	Disables debugging of the FMCHS options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable FMCHS event debugging:

```
(Cisco Controller) >debug fmchs event enable
```

debug flexconnect client ap

To debug FlexConnect client access point MAC addresses, use the **debug flexconnect client ap** command.

debug flexconnect client ap *ap-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

Syntax Description

add	Adds the MAC address to the group.
delete	Deletes the MAC address from the group.
MAC-address	MAC address of the client

Command Default

None

Command History

Release	Modification
8.1	This command was added

The following example shows how to debug FlexConnect client ap 'room' MAC addresses:

```
(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

To configure debug logging of the syslog server for a FlexConnect client AP, use the **debug flexconnect client ap** command.

debug flexconnect client ap *ap-name* **syslog** {*ip-address* | **disable**}

Syntax Description

ip-address	Configures the syslog server ip-address for debug logging.
disable	Disables the debug logging to the syslog server.

Command Default

None

Command History

Release	Modification
8.1	This command was added.

The following example shows how to configure syslog server for debug log for the FlexConnect client AP 'room':

```
(Cisco Controller) >debug flexconnect client ap room syslog 192.168.1.1
```

debug flexconnect client group

To debug FlexConnect client group MAC addresses, use the **debug flexconnect client group** command.

debug flexconnect client group *group-name* {**add** | **delete**} *MAC-address1 MAC-address2 MAC-address3 MAC-address4*

Syntax Description

add	Adds the MAC address to the group.
delete	Deletes the MAC address from the group.
MAC-address	MAC address of the client.

Command Default

None

Command History

Release	Modification
8.1	This command was added.

The following example shows how to debug FlexConnect client group MAC addresses:

```
(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

To debug FlexConnect group access point syslog, use the **debug flexconnect client group** command.

debug flexconnect client group *group-name* **syslog** *ip-address* | *disable*

Syntax Description

ip-address	Configures the syslog server ip-address for debug logging.
disable	Disables the debug logging to the syslog server.

Command Default

None

Command History

Release	Modification
8.1	This command was added.

The following example shows how to configure FlexConnect client group 'school' for debug logging purposes:

```
(Cisco Controller) >debug flexconnect client group school syslog 192.168.1.1
```

debug flexconnect group

To configure debugging of FlexConnect access point groups, use the **debug flexconnect group** command.

debug flexconnect group {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of FlexConnect access point groups.
disable	Disables the debugging of FlexConnect access point groups.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of FlexConnect access point groups:

```
(Cisco Controller) >debug flexconnect group enable
```

debug ft

To configure debugging of 802.11r, use the **debug ft** command.

debug ft {**events** | **keys**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of the 802.11r events.
keys	Configures debugging of the 802.11r keys.
enable	Enables debugging of the 802.11r options.
disable	Disables debugging of the 802.11r options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable 802.11r debugging:

```
(Cisco Controller) >debug ft events enable
```

debug hotspot

To configure debugging of HotSpot events or packets, use the **debug hotspot** command.

debug hotspot {**events** | **packets**} {**enable** | **disable**} {**enable** | **disable**}

Syntax Description

events	Configures debugging of HotSpot events.
packets	Configures debugging of HotSpot packets.
enable	Enables the debugging of HotSpot options.
disable	Disables the debugging of HotSpot options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of hotspot events:

```
(Cisco Controller) >debug hotspot events enable
```

debug ipv6

To configure debugging of IPv6 options, use the **debug ipv6** command.

debug ipv6 {**all** | **bt** | **classifier** | **errors** | **events** | **filter** | **fsm** | **gleaner** | **hwapi** | **memory** | **ndsuppress** | **parser** | **policy** | **ra_throttler** | **switcher**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all the IPv6 information.
bt	Configures debugging of the IPv6 neighbor binding table.
classifier	Configures debugging of the IPv6 packet classifiers.
errors	Configures debugging of the IPv6 errors.
events	Configures debugging of the IPv6 events.
filter	Configures filters for the IPv6 debugs.
fsm	Configures debugging of the IPv6 finite state machine (FSM).
gleaner	Configures debugging of the IPv6 gleaner. Learning of entries is called gleaning.
hwapi	Configures debugging of the IPv6 hardware APIs.
memory	Configures debugging of the IPv6 binding table memory usage.
ndsuppress	Configures debugging of the suppressed IPv6 neighbor discoveries.
parser	Configures debugging of the IPv6 parser.
policy	Configures debugging of the IPv6 policies.
ra_throttler	Configures debugging of the IPv6 router advertising throttler.
switcher	Configures debugging of the IPv6 switcher.
enable	Enables debugging of the IPv6 options.
disable	Disables debugging of the IPv6 options.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of IPv6 policies:

```
(Cisco Controller) >debug ipv6 policy enable
```

Debug Commands: j to q

- debug l2age, on page 1312
- debug mac, on page 1313
- debug mdns all, on page 1314
- debug mdns detail , on page 1315
- debug mdns error , on page 1316
- debug mdns message , on page 1317
- debug mdns ha, on page 1318
- debug memory, on page 1319
- debug mesh security, on page 1320
- debug mobility, on page 1321
- debug nac, on page 1323
- debug nmsp, on page 1324
- debug ntp, on page 1325
- debug packet error, on page 1326
- debug packet logging, on page 1327
- debug pem, on page 1330
- debug pm, on page 1331
- debug poe, on page 1333
- debug policy, on page 1334
- debug profiling, on page 1335

debug l2age

To configure the debugging of Layer 2 age timeout messages, use the **debug l2age** command.

debug l2age {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of Layer2 age settings.
disable	Disables the debugging Layer2 age settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of Layer2 age settings:

```
(Cisco Controller) > debug l2age enable
```

Related Commands

debug disable-all

debug mac

To configure the debugging of the client MAC address, use the **debug mac** command.

debug mac {**disable** | **addr** *MAC*}

Syntax Description

disable	Disables the debugging of the client using the MAC address.
addr	Configures the debugging of the client using the MAC address.
MAC	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of the client using the MAC address:

```
(Cisco Controller) > debug mac addr 00.0c.41.07.33.a6
```

Related Commands

debug disable-all

debug mdns all

To debug all multicast DNS (mDNS) messages, details, and errors, use the **debug mdns all** command.

debug mdns all {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of all mDNS messages, details, and errors.
disable	Disables the debugging of all mDNS messages, details, and errors.

Command Default

By default, the debugging of all mDNS messages, details, and errors is disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable debugging of all mDNS messages, details, and errors:

```
(Cisco Controller) > debug mdns all enable
```

Related Commands

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

To debug multicast DNS (mDNS) details, use the **debug mdns detail** command.

debug mdns detail {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS details.
disable	Disables the debugging of mDNS details.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS details:

```
(Cisco Controller) > debug mdns detail enable
```

Related Commands

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

To debug multicast DNS (mDNS) errors, use the **debug mdns error** command.

debug mdns error {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS errors.
disable	Disables the debugging of mDNS errors.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS errors.

```
(Cisco Controller) > debug mdns error enable
```

Related Commands

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

To debug multicast DNS (mDNS) messages, use the **debug mdns message** command.

debug mdns message {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of mDNS messages.
disable	Disables the debugging of mDNS messages.

Command Default

Disabled.

Command History

Release	Modification
7.4	This command was introduced.

The following example shows how to enable the debugging of mDNS messages:

```
(Cisco Controller) > debug mdns message enable
```

Related Commands

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

To debug all the multicast Domain Name System (mDNS) High Availability (HA) messages, use the **debug mdns ha** command.

debug mdns ha {**enable** | **disable**}

Syntax Description

enable	Enables debugging of all the mDNS HA messages.
disable	Disables debugging of all the mDNS HA messages.

Command Default

This command is disabled by default.

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

This command is automatically enabled when the **debug mdns all** command is enabled.

The following example shows how to enable debugging of all the mDNS HA messages:

```
(Cisco Controller) > debug mdns ha enable
```

debug memory

To enable or disable the debugging of errors or events during the memory allocation of the controller, use the **debug memory** command.

debug memory { **errors** | **events** } { **enable** | **disable** }

Syntax Description

errors	Configures the debugging of memory leak errors.
events	Configures debugging of memory leak events.
enable	Enables the debugging of memory leak events.
disable	Disables the debugging of memory leak events.

Command Default

By default, the debugging of errors or events during the memory allocation of the controller is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of memory leak events:

```
(Cisco Controller) > debug memory events enable
```

Related Commands

config memory monitor errors

show memory monitor

config memory monitor leaks

debug mesh security

To configure the debugging of mesh security issues, use the **debug mesh security** command.

debug mesh security {**all** | **events** | **errors**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all mesh security messages.
events	Configures the debugging of mesh security event messages.
errors	Configures the debugging of mesh security error messages.
enable	Enables the debugging of mesh security error messages.
disable	Disables the debugging of mesh security error messages.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of mesh security error messages:

```
(Cisco Controller) >debug mesh security errors enable
```

debug mobility

To configure the debugging of wireless mobility, use the **debug mobility** command.

debug mobility {**ap-list** | **config** | **directory** | **dtls** | **handoff** | **keep-alive** | **multicast** | **oracle** | **packet** | **peer-ip** *IP-address* | **pmk** | **pmtu-discovery** | **redha**} {**enable** | **disable**}

Syntax Description

ap-list	Configures the debugging of wireless mobility access point list.
config	Configures the debugging of wireless mobility configuration.
directory	Configures the debugging of wireless mobility error messages.
dtls	Configures the debugging of wireless mobility Datagram Transport Layer Security (DTLS) options.
handoff	Configures the debugging of wireless mobility handoff messages.
keep-alive	Configures the debugging of wireless mobility CAPWAP data DTLS keep-alive packets.
multicast	Configures the debugging of multicast mobility packets.
oracle	Starts the debugging of wireless mobility oracle options.
packet	Configures the debugging of wireless mobility packets.
peer-ip	Configures IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
IP-address	IP address of the mobility peer for which incoming and outgoing mobility messages should be displayed.
pmk	Configures the debugging of wireless mobility pairwise master key (PMK).
pmtu-discovery	Configures the debugging of the wireless mobility path MTU discovery.
redha	Configures the debugging of the multicast mobility high availability.

enable	Enables the debugging of the wireless mobility feature.
disable	Disables the debugging of the wireless mobility feature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to enable the debugging of wireless mobility packets.

```
(Cisco Controller) >debug mobility handoff enable
```

debug nac

To configure the debugging of Network Access Control (NAC), use the **debug nac** command.

debug nac {**events** | **packet**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of NAC events.
packet	Configures the debugging of NAC packets.
enable	Enables the NAC debugging.
disable	Disables the NAC debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of NAC settings:

```
(Cisco Controller) > debug nac events enable
```

Related Commands

show nac statistics

show nac summary

config guest-lan nac

config wlan nac

debug nmsp

To configure the debugging of the Network Mobility Services Protocol (NMSP), use the **debug nmsp** command.

debug nmsp {**all** | **connection** | **detail** | **error** | **event** | **message** | **packet**}

Syntax Description

all	Configures the debugging for all NMSP messages.
connection	Configures the debugging for NMSP connection events.
detail	Configures the debugging for NMSP events in detail.
error	Configures the debugging for NMSP error messages.
event	Configures the debugging for NMSP events.
message	Configures the debugging for NMSP transmit and receive messages.
packet	Configures the debugging for NMSP packet events.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of NMSP connection events:

```
(Cisco Controller) > debug nmsp connection
```

Related Commands

clear nmsp statistics

debug disable-all

config nmsp notify-interval measurement

debug ntp

To configure the debugging of the Network Time Protocol (NTP), use the **debug ntp** command.

debug ntp {**detail** | **low** | **packet**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of detailed NTP messages.
low	Configures the debugging of NTP messages.
packet	Configures the debugging of NTP packets.
enable	Enables the NTP debugging.
disable	Disables the NTP debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of NTP settings:

```
(Cisco Controller) > debug ntp packet enable
```

Related Commands

debug disable-all

debug packet error

To configure debugging of the packets sent to the controller CPU , use the **debug packet error** command.

debug packet error {**enable** | **disable**}

Syntax Description

enable	Enables debugging of the packets sent to the controller CPU.
disable	Disables debugging of the packets sent to the controller CPU.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the packets sent to the controller CPU:

```
(Cisco Controller) > debug packet error enable
```

debug packet logging

To configure logging of the packets sent to the controller CPU, use the **debug packet logging** command.

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*}

Syntax Description

acl	Filters the displayed packets according to a rule.
disable	Disables logging of all the packets.
enable	Enables logging of all the packets.
rx	Displays all the received packets.
tx	Displays all the transmitted packets.
all	Displays both the transmitted and the received packets.
packet_count	Maximum number of packets to be logged. The range is from 1 to 65535. The default value is 25.
display_size	Number of bytes to be displayed when printing a packet. By default, the entire packet is displayed.
format	Configures the format of the debug output.
hex2pcap	Configures the output format to be compatible with the hex2pcap format. The standard format used by Cisco IOS supports the use of hex2pcap and can be decoded using an HTML front end.
text2pcap	Configures the output format to be compatible with the text2pcap format. In this format, the sequence of packets can be decoded from the same console log file. .
clear-all	Clears all the existing rules pertaining to the packets.
driver	Filters the packets based on an incoming port or a Network Processing Unit (NPU) encapsulation type.
rule_index	Index of the rule that is a value between 1 and 6 (inclusive).
action	Action for the rule, which can be **permit**, **deny**, or **disable**.

npu_encap	NPU encapsulation type that determines how the packets are filtered. The possible values are *dhcp, dot11-mgmt, dot11-probe, dot1x, eoip-ping, iapp, ip, lwapp, multicast, orphan-from-sta, orphan-to-sta, rbcp, wired-guest,* or *any*.
port	Physical port for packet transmission or reception.
eoip-eth	Filters packets based on the Ethernet II header in the Ethernet over IP (EoIP) payload.
dst	Destination MAC address.
src	Source MAC address.
type	Two-byte type code, such as 0x800 for IP, 0x806 for Address Resolution Protocol (ARP). You can also enter a few common string values such as *ip* (for 0x800) or *arp* (for 0x806).
vlan	Two-byte VLAN identifier.
eoip-ip	Filters packets based on the IP header in the EoIP payload.
proto	Protocol. Valide values are: *ip, icmp, igmp, ggp, ipencap, st, tcp, egp, pup, udp, hmp, xns-idp, rdp, iso-tp4, xtp, ddp, idpr-cmtp, rspf, vmtp, ospf, ipip,* and *encap*.
src_port	User Datagram Protocol or Transmission Control Protocol (UDP or TCP) two-byte source port, such as *telnet, 23* , or *any*. The controller supports the following strings: *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,* and *hmmp-ind*.
dst_port	UDP or TCP two-byte destination port, such as *telnet, 23*, or *any*. The controller supports the same strings as those for the src_port.
eth	Filters packets based on the values in the Ethernet II header.
ip	Filters packets based on the values in the IP header.
lwapp-dot11	Filters packets based on the 802.11 header in the Lightweight Access Point Protocol (LWAPP) payload.
bssid	Basic Service Set Identifier of the VLAN.
lwapp-ip	Filters packets based on the IP header in the LWAPP payload.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable logging of a packet:

```
(Cisco Controller) > debug packet logging enable
```

debug pem

To configure debugging of the access policy manager, use the **debug pem** command.

debug pem {**events** | **state**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of the policy manager events.
state	Configures the debugging of the policy manager state machine.
enable	Enables the debugging of the access policy manager.
disable	Disables the debugging of the access policy manager.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of the access policy manager:

```
(Cisco Controller) >debug pem state enable
```

debug pm

To configure the debugging of the security policy manager module, use the **debug pm** command.

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**}}

Syntax Description

all disable	Disables all debugging in the policy manager module.
config	Configures the debugging of the policy manager configuration.
hwcrypto	Configures the debugging of hardware offload events.
ikemsg	Configures the debugging of Internet Key Exchange (IKE) messages.
init	Configures the debugging of policy manager initialization events.
list	Configures the debugging of policy manager list mgmt.
message	Configures the debugging of policy manager message queue events.
pki	Configures the debugging of Public Key Infrastructure (PKI) related events.
rng	Configures the debugging of random number generation.
rules	Configures the debugging of Layer 3 policy events.
sa-export	Configures the debugging of SA export (mobility).
sa-import	Configures the debugging of SA import (mobility).
ssh-l2tp	Configures the debugging of policy manager Layer 2 Tunneling Protocol (l2TP) handling.
ssh-appgw	Configures the debugging of application gateways.
ssh-engine	Configures the debugging of the policy manager engine.
ssh-int	Configures the debugging of the policy manager intercepter.
ssh-pmgr	Configures the debugging of the policy manager.

ssh-ppp	Configures the debugging of policy manager Point To Point Protocol (PPP) handling.
ssh-tcp	Configures the debugging of policy manager TCP handling.
enable	Enables the debugging.
disable	Disables the debugging.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the debugging of PKI-related events:

```
(Cisco Controller) > debug pm pki enable
```

Related Commands

debug disable-all

debug poe

To configure the debugging of Power over Ethernet (PoE), use the **debug poe** command.

debug poe {**detail** | **message** | **error**} {**enable** | **disable**}

Syntax Description

detail	Configures the debugging of PoE detail logs.
error	Configures the debugging of PoE error logs.
message	Configures the debugging of PoE messages.
enable	Enables the debugging of PoE logs.
disable	Disables the debugging of PoE logs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the PoE debugging:

```
(Cisco Controller) > debug poe message enable
```

Related Commands

debug disable-all

debug policy

To configure debugging of policy settings, use the **debug policy** command.

debug policy {**errors** | **events**} {**enable** | **disable**}

Syntax Description

errors	Configures debugging of policy errors.
events	Configures debugging of policy events.
enable	Enables debugging of policy events.
disable	Disables debugging of policy events.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of policy errors:

```
(Cisco Controller) >  debug policy errors enable
```

debug profiling

To configure the debugging of client profiling, use the **debug profiling** command.

debug profiling {**enable** | **disable**}

Syntax Description

enable	Enables the debugging of client profiling (HTTP and DHCP profiling).
disable	Disables the debugging of client profiling (HTTP and DHCP profiling).

Command Default

Disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of client profiling:

```
(Cisco Controller) >debug profiling enable
```

Debug Commands: r to z

- debug rbcp, on page 1338
- debug rfid, on page 1339
- debug snmp, on page 1340
- debug transfer, on page 1341
- debug voice-diag, on page 1342
- debug wcp, on page 1343
- debug web-auth, on page 1344
- debug wips, on page 1345
- debug wps sig, on page 1346
- debug wps mfp, on page 1347

debug rbcp

To configure Router Blade Control (RBCP) debug options, use the **debug rbcp** command.

debug rbcp {**all** | **detail** | **errors** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of RBCP.
detail	Configures the debugging of RBCP detail.
errors	Configures the debugging of RBCP errors.
packet	Configures the debugging of RBCP packet trace.
enable	Enables the RBCP debugging.
disable	Disables the RBCP debugging.

Command Default

None

The following example shows how to enable the debugging of RBCP settings:

```
(Cisco Controller) > debug rbcp packet enable
```

Related Commands

debug disable-all

debug rfid

To configure radio frequency identification (RFID) debug options, use the **debug rfid** command.

debug rfid {**all** | **detail** | **errors** | **nmsp** | **receive**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all RFID.
detail	Configures the debugging of RFID detail.
errors	Configures the debugging of RFID error messages.
nmsp	Configures the debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures the debugging of incoming RFID tag messages.
enable	Enables the RFID debugging.
disable	Disables the RFID debugging.

Command Default

None

The following example shows how to enable the debugging of RFID error messages:

```
(Cisco Controller) > debug rfid errors enable
```

Related Commands

debug disable-all

debug snmp

To configure SNMP debug options, use the **debug snmp** command.

debug snmp {**agent** | **all** | **mib** | **trap**} {**enable** | **disable**}

Syntax Description

agent	Configures the debugging of the SNMP agent.
all	Configures the debugging of all SNMP messages.
mib	Configures the debugging of the SNMP MIB.
trap	Configures the debugging of SNMP traps.
enable	Enables the SNMP debugging.
disable	Disables the SNMP debugging.

Command Default

None

The following example shows how to enable the SNMP debugging:

```
(Cisco Controller) > debug snmp trap enable
```

Related Commands

debug disable-all

debug transfer

To configure transfer debug options, use the **debug transfer** command.

debug transfer {**all** | **tftp** | **trace**} {**enable** | **disable**}

Syntax Description

all	Configures the debugging of all transfer messages.
tftp	Configures the debugging of TFTP transfers.
trace	Configures the debugging of transfer messages.
enable	Enables the debugging of transfer messages.
disable	Disables the debugging of transfer messages.

Command Default

None

The following example shows how to enable the debugging of transfer messages:

```
(Cisco Controller) > debug transfer trace enable
```

Related Commands

debug disable-all

debug voice-diag

To trace call or packet flow, use the **debug voice-diag** command.

debug voice-diag {**enable** *client_mac1* [*client_mac2*] [**verbose**] | **disable**}

Syntax Description

enable	Enables the debugging of voice diagnostics for voice clients involved in a call.
client_mac1	MAC address of a voice client.
client_mac2	(Optional) MAC address of an additional voice client. **Note** Voice diagnostics can be enabled or disabled for a maximum of two voice clients at a time.
verbose	(Optional) Enables debug information to be displayed on the console. **Note** When voice diagnostics is enabled from the NCS or Prime Infrastructure, the verbose option is not available.
disable	Disables the debugging of voice diagnostics for voice clients involved in a call.

Command Default

None

Usage Guidelines

Follow these guidelines when you use the **debug voice-diag** command:

- When the command is entered, the validity of the clients is not checked.
- A few output messages of the command are sent to the NCS or Prime Infrastructure.
- The command expires automatically after 60 minutes.
- The command provides the details of the call flow between a pair of client MACs involved in an active call.

Note Voice diagnostics can be enabled for a maximum of two voice clients at a time.

The following example shows how to enable transfer/upgrade settings:

```
(Cisco Controller) > debug voice-diag enable 00:1a:a1:92:b9:5c 00:1a:a1:92:b5:9c verbose
```

Related Commands

show client voice-diag

show client calls

debug wcp

To configure the debugging of WLAN Control Protocol (WCP), use the **debug wcp** command.

debug wcp {**events** | **packet**} {**enable** | **disable**}

Syntax Description

events	Configures the debugging of WCP events.
packet	Configures the debugging of WCP packets.
enable	Enables the debugging of WCP settings.
disable	Disables the debugging of WCP settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WCP settings:

```
(Cisco Controller) >debug wcp packet enable
```

debug web-auth

To configure debugging of web-authenticated clients, use the **debug web-auth** command.

debug web-auth {**redirect** { **enable mac** *mac_address* | **disable**} | **webportal-server** {**enable** | **disable**} }

Syntax Description

redirect	Configures debugging of web-authenticated and redirected clients.
enable	Enables the debugging of web-authenticated clients.
mac	Configures the MAC address of the web-authenticated client.
mac_address	MAC address of the web-authenticated client.
disable	Disables the debugging of web-authenticated clients.
webportal-server	Configures the debugging of portal authentication of clients.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of a web authenticated and redirected client:

```
(Cisco Controller) > debug web-auth redirect enable mac xx:xx:xx:xx:xx:xx
```

debug wips

To configure debugging of wireless intrusion prevention system (WIPS), use the **debug wips** command.

debug wips {**all** | **error** | **event** | **nmsp** | **packet**} {**enable** | **disable**}

Syntax Description

all	Configures debugging of all WIPS messages.
error	Configures debugging of WIPS errors.
event	Configures debugging of WIPS events.
nmsp	Configures debugging of WIPS Network Mobility Services Protocol (NMSP) events.
packet	Configures debugging of WIPS packets.
enable	Enables debugging of WIPS.
disable	Disables debugging of WIPS.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable debugging of all WIPS messages:

```
(Cisco Controller) > debug wips all enable
```

Related Commands

debug client

debug dot11 rogue

show wps summary

show wps wips

debug wps sig

To configure the debugging of Wireless Provisioning Service (WPS) signature settings, use the **debug wps sig** command.

debug wps sig {**enable** | **disable**}

Syntax Description

enable	Enables the debugging for WPS settings.
disable	Disables the debugging for WPS settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WPS signature settings:

```
(Cisco Controller) > debug wps sig enable
```

Related Commands

debug wps mfp

debug disable-all

debug wps mfp

To configure the debugging of WPS Management Frame Protection (MFP) settings, use the **debug wps mfp** command.

debug wps mfp {**client** | **capwap** | **detail** | **report** | **mm**} {**enable** | **disable**}

Syntax Description

client	Configures the debugging for client MFP messages.
capwap	Configures the debugging for MFP messages between the controller and access points.
detail	Configures the detailed debugging for MFP messages.
report	Configures the debugging for MFP reporting.
mm	Configures the debugging for MFP mobility (inter-controller) messages.
enable	Enables the debugging for WPS MFP settings.
disable	Disables the debugging for WPS MFP settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the debugging of WPS MFP settings:

```
(Cisco Controller) > debug wps mfp detail enable
```

Related Commands

debug disable-all

debug wps sig

PART V

IMM Commands

- IMM Commands, on page 1351

IMM Commands

- imm address, on page 1352
- imm dhcp, on page 1353
- imm mode, on page 1354
- imm restart, on page 1355
- imm summary, on page 1356
- imm username, on page 1357

imm address

To configure the static IP address of the IMM, use the **imm address** command.

imm address *ip-addr netmask gateway*

Syntax Description

ip-addr	IP address of the IMM
netmask	Netmask of the IMM
gateway	Gateway of the IMM

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

The following example shows how to set the static IP address of an IMM:

```
(Cisco Controller) >imm address 209.165.200.225 255.255.255.224 10.1.1.1
```

imm dhcp

To configure DHCP for the IMM, use the **imm dhcp** command.

imm dhcp {**enable** | **disable** | **fallback**}

Syntax Description

enable	Enables DHCP for the IMM
disable	Disables DHCP for the IMM
fallback	Enables DHCP for the IMM, but if it fails, then uses static IP of the IMM

Command Default

DHCP for IMM is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable DHCP for the IMM:

```
(Cisco Controller) >imm dhcp enable
```

imm mode

To configure the IMM mode, use the **imm mode** command.

imm mode {**shared** | **dedicated**}

Syntax Description

shared	Sets IMM in shared mode
dedicated	Sets IMM in dedicated mode

Command Default

Dedicated

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the IMM in shared mode:

```
(Cisco Controller) >imm mode
```

imm restart

To restart the IMM, use the **imm restart** command.

imm restart

Syntax Description		
	restart	Saves your settings and restarts the IMM

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

imm summary

To view the IMM parameters, use the **imm summary** command.

imm summary

Syntax Description

summary	Lists the IMM parameters

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows a typical summary of the IMM:

```
(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

To configure the logon credentials for an IMM user, use the **imm username** command.

imm username *username password*

Syntax Description

username	Username for the user
password	Password for the user

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the logon credentials of an IMM user:

```
(Cisco Controller) >imm username username1 password1
```

PART VI

License Commands

- License Commands, on page 1361

License Commands

- license activate ap-count eval, on page 1362
- license activate feature, on page 1363
- license add ap-count, on page 1364
- license add feature, on page 1365
- license clear, on page 1366
- license comment, on page 1367
- license deactivate ap-count eval, on page 1368
- license deactivate feature, on page 1369
- license delete ap-count, on page 1370
- license delete feature, on page 1371
- license install, on page 1372
- license modify priority, on page 1373
- license revoke, on page 1375
- license save, on page 1376
- license smart, on page 1377

license activate ap-count eval

To activate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate ap-count eval** command.

license activate ap-count eval

Syntax Description

This command has no arguments or keywords.

Command Default

By default, in release 7.3 Cisco Flex 7500 Series Controllers and Cisco 8500 Series Wireless LAN Controllers support 6000 APs.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you activate this license, the controller prompts you to accept or reject the End User License Agreement (EULA) for the given license. If you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

The following example shows how to activate an evaluation AP-count license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license activate ap-count eval
```

license activate feature

To activate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license activate feature** command.

license activate feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to activate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license activate feature data-DTLS
```

license add ap-count

To configure the number of access points (APs) that an AP license can support on Cisco Flex 7500 and 8500 Series Wireless LAN controllers, use the **license add ap-count** command.

license add ap-count *count*

Syntax Description

count	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Right to Use (RTU) licensing allows you to enable a desired AP license count on the controller after accepting the End User License Agreement (EULA). You can now easily add AP counts on a controller without using external tools. RTU licensing is available only on Cisco Flex 7500 and 8500 series Wireless LAN controllers.

You can use this command to increase the count of an existing AP license. When you activate a license that supports a smaller number of APs than the current number of APs connected to the controller, the activation command fails.

The following example shows how to configure the count of an AP license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license add ap-count 5000
```

license add feature

To add a license for a feature on the Cisco 5520 Wireless Controller, Cisco Flex 7510 Wireless Controller, Cisco 8510 Wireless Controller, Cisco 8540 Wireless Controller, and Cisco Virtual Controller, use the **license add feature** command.

license add feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters. For example, data_encryption.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6. This command is applicable to Cisco Flex 7510 Wireless Controller and Cisco 8510 Wireless Controller.
8.1	This command is applicable to Cisco 5520 Wireless Controller, Cisco Flex 7510 Wireless Controller, Cisco 8510 Wireless Controller, Cisco 8540 Wireless Controller, and Cisco vWLC.

The following example shows how to add a data_encryption feature license:

```
(Cisco Controller) > license add feature data_encryption
```

license clear

To remove a license from the Cisco 5500 Series Controller, use the **license clear** command.

license clear *license_name*

Syntax Description

license_name	Name of the license.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can delete an expired evaluation license or any unused license. You cannot delete unexpired evaluation licenses, the permanent base image license, or licenses that are in use by the controller.

The following example shows how to remove the license settings of the license named wplus-ap-count:

```
(Cisco Controller) > license clear wplus-ap-count
```

license comment

To add comments to a license or delete comments from a license on the Cisco 5500 Series Controller, use the **license comment** command.

license comment {**add** | **delete**} *license_name comment_string*

Syntax Description

add	Adds a comment.
delete	Deletes a comment.
license_name	Name of the license.
comment_string	License comment.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to add a comment “wplus ap count license” to the license name wplus-ap-count:

```
(Cisco Controller) > license comment add wplus-ap-count Comment for wplus ap count license
```

license deactivate ap-count eval

To deactivate an evaluation access point license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license deactivate ap-count eval** command.

license deactivate ap-count eval

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deactivate an evaluation AP license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license deactivate ap-count eval
```

license deactivate feature

To deactivate a feature license on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license deactivate feature** command.

license deactivate feature *license_name*

Syntax Description

license_name	Name of the feature license. The license name can be up to 50 case-sensitive characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to deactivate a data DTLS feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license deactivate feature data_DTLS
```

license delete ap-count

To delete an access point (AP) count license on the Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN Controllers, use the **license delete ap-count** command.

license delete ap-count *count*

Syntax Description

count	Number of APs that the AP license supports. The range is from 1 to the maximum number of APs that the controller can support. The count must be a multiple of 5.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete an AP count license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license delete ap-count 5000
```

license delete feature

To delete a license for a feature on Cisco Flex 7500 Series and Cisco 8500 Series Wireless LAN controllers, use the **license delete feature** command.

license delete feature *license_name*

Syntax Description

license_name	Name of the feature license.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to delete the High Availability feature license on a Cisco Flex 7500 Series controller:

```
(Cisco Controller) > license delete feature high_availability
```

license install

To install a license on the Cisco 5500 Series Controller, use the **license install** command.

license install *url*

Syntax Description

url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

We recommend that the access point count be the same for the base-ap-count and wplus-ap-count licenses installed on your controller. If your controller has a base-ap-count license of 100 and you install a wplus-ap-count license of 12, the controller supports up to 100 access points when the base license is in use but only a maximum of 12 access points when the wplus license is in use.

You cannot install a wplus license that has an access point count greater than the controller's base license. For example, you cannot apply a wplus-ap-count 100 license to a controller with an existing base-ap-count 12 license. If you attempt to register for such a license, an error message appears indicating that the license registration has failed. Before upgrading to a wplus-ap-count 100 license, you would first have to upgrade the controller to a base-ap-count 100 or 250 license.

The following example shows how to install a license on the controller from the URL tftp://10.10.10.10/path/license.lic:

```
(Cisco Controller) > license install tftp://10.10.10.10/path/license.lic
```

license modify priority

To raise or lower the priority of the base-ap-count or wplus-ap-count evaluation license on a Cisco 5500 Series Controller, use the **license modify priority** command.

license modify priority *license_name* {**high** | **low**}

Syntax Description

license_name	Ap-count evaluation license.
high	Modifies the priority of an ap-count evaluation license.
low	Modifies the priority of an ap-count evaluation license.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If you are considering upgrading to a license with a higher access point count, you can try an evaluation license before upgrading to a permanent version of the license. For example, if you are using a permanent license with a 50 access point count and want to try an evaluation license with a 100 access point count, you can try out the evaluation license for 60 days.

AP-count evaluation licenses are set to low priority by default so that the controller uses the ap-count permanent license. If you want to try an evaluation license with an increased access point count, you must change its priority to high. If you no longer want to have this higher capacity, you can lower the priority of the ap-count evaluation license, which forces the controller to use the permanent license.

Note You can set the priority only for ap-count evaluation licenses. AP-count permanent licenses always have a medium priority, which cannot be configured.

Note If the ap-count evaluation license is a wplus license and the ap-count permanent license is a base license, you must also change the feature set to wplus.

Note To prevent disruptions in operation, the controller does not switch licenses when an evaluation license expires. You must reboot the controller in order to return to a permanent license. Following a reboot, the controller defaults to the same feature set level as the expired evaluation license. If no permanent license at the same feature set level is installed, the controller uses a permanent license at another level or an unexpired evaluation license.

The following example shows how to set the priority of the wplus-ap-count to high:

```
(Cisco Controller) > license modify priority wplus-ap-count high
```

license revoke

To rehost a license on a Cisco 5500 Series Wireless Controller, use the **license revoke** command.

license revoke {*permission_ticket_url* | **rehost** *rehost_ticket_url*}

Syntax Description

permission_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the permission ticket.
rehost	Specifies the rehost license settings.
rehost_ticket_url	URL of the TFTP server (tftp://server_ip/path/filename) where you saved the rehost ticket.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Before you revoke a license, save the device credentials by using the **license save credential** *url* command.

You can rehost all permanent licenses except the permanent base image license. Evaluation licenses and the permanent base image license cannot be rehosted.

In order to rehost a license, you must generate credential information from the controller and use it to obtain a permission ticket to revoke the license from the Cisco licensing site, https://tools.cisco.com/SWIFT/LicensingUI/Quickstart. Next, you must obtain a rehost ticket and use it to obtain a license installation file for the controller on which you want to install the license.

For detailed information on rehosting licenses, see the "Installing and Configuring Licenses" section in the *Cisco Wireless LAN Controller Configuration Guide*.

The following example shows how to revoke the license settings from the saved permission ticket URL tftp://10.10.10.10/path/permit_ticket.lic:

```
(Cisco Controller) > license revoke tftp://10.10.10.10/path/permit_ticket.lic
```

The following example shows how to revoke the license settings from the saved rehost ticket URL tftp://10.10.10.10/path/rehost_ticket.lic:

```
(Cisco Controller) > license revoke rehost tftp://10.10.10.10/path/rehost_ticket.lic
```

license save

To save a backup copy of all installed licenses or license credentials on the Cisco 5500 Series Controller, use the **license save** command.

license save *credential url*

Syntax Description

credential	Device credential information.
url	URL of the TFTP server (tftp://server_ip/path/filename).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Save the device credentials before you revoke the license by using the **license revoke** command.

The following example shows how to save a backup copy of all installed licenses or license credentials on tftp://10.10.10.10/path/cred.lic:

```
(Cisco Controller) > license save credential tftp://10.10.10.10/path/cred.lic
```

license smart

To register or deregister a device using Cisco Smart Software Licensing platform, use the **license smart** command.

license smart {**register** | **deregister**} *idtoken*

Syntax Description

register	To add and activate a device on Cisco Smart Software License platform
deregister	To delete a device on Cisco Smart Software License platform
idtoken	unique id for the device

Command History

Release	Modification
8.2	This command was introduced.

The following example shows how to register a device on Cisco Smart Software License platform:

```
(Cisco Controller) > license smart register
RkMxJbjKMV11hmpgh46mAgXSNKmticyJzu0xDfYgf8xflkiYbZsCqprt
```

PART VII

Show Commands

- Show Commands: 802.11, on page 1381
- Show Commands: a to i, on page 1397
- Show Commands: j to q, on page 1607
- Show Commands: r to z, on page 1725

Show Commands: 802.11

- show 802.11, on page 1382
- show 802.11, on page 1384
- show 802.11 cleanair, on page 1386
- show 802.11 cleanair air-quality summary, on page 1388
- show 802.11 cleanair air-quality worst, on page 1389
- show 802.11 cleanair device ap, on page 1390
- show 802.11 cleanair device type, on page 1391
- show 802.11 cu-metrics, on page 1393
- show 802.11 extended, on page 1394
- show 802.11 media-stream, on page 1395

show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

show 802.11 {**a** | **b** | **h**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.

Command Default

None.

This example shows to display basic 802.11a network settings:

```
> 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
```

This example shows how to display basic 802.11h network settings:

```
> show 802.11h
802.11h ..................................... powerconstraint : 0
802.11h ..................................... channelswitch : Disable
802.11h ..................................... channelswitch mode : 0
```

Related Commands

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show 802.11

To display basic 802.11a, 802.11b/g, or 802.11h network settings, use the **show 802.11** command.

show 802.11 {**a** | **b** | **h**}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.

Command Default

None.

This example shows to display basic 802.11a network settings:

```
> 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
```

This example shows how to display basic 802.11h network settings:

```
> show 802.11h
802.11h ..................................... powerconstraint : 0
802.11h ..................................... channelswitch : Disable
802.11h ..................................... channelswitch mode : 0
```

Related Commands

show ap stats

show ap summary

show client summary

show network

show network summary

show port

show wlan

show 802.11 cleanair

To display the multicast-direct configuration state, use the **show 802.11 cleanair** command.

show 802.11{**a** | **b** | **h**} **cleanair config**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
config	Displays the network Cleanair configuration.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the 802.11a cleanair configuration:

```
(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

To display the air quality summary information for the 802.11 networks, use the **show 802.11 cleanair air-quality summary** command.

show 802.11 {**a** | **b** | **h**} **cleanair air-quality summary**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
summary	Displays a summary of 802.11 radio band air quality information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the air quality information for the 802.11a network:

```
(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

To display the worst air quality information for the 802.11 networks, use the **show 802.11 cleanair air-quality worst** command.

show 802.11{**a** | **b** | **h**} **cleanair air-quality worst**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
worst	Displays the worst air quality information for 802.11 networks.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display worst air quality information for the 802.11a network:

```
(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

To display the information of the device access point on the 802.11 radio band, use the **show 802.11 cleanair device ap** command.

show 802.11 {**a** | **b** | **h**} **cleanair device ap** *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
cisco_ap	Specified access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the device access point for the 802.11a network:

```
(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

To display the information of all the interferers device type detected by a specific access point on the 802.11 radio band, use the **show 802.11 cleanair device type** command.

show 802.11{**a** | **b** | **h**} **cleanair device type** *device_type*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
device_type	Interferer device type for a specified radio band. The device type is one of the following: • tdd-tx—Tdd-transmitter device information. • jammer—Jammer device information. • cont-tx—Continuous-transmitter devices information. • dect-like—Dect-like phone devices information. • video—Video devices information. • 802.11-inv—WiFi inverted devices information. • 802.11-nonstd—Nonstandard WiFi devices information. • superag—Superag devices information. • canopy—Canopy devices information. • wimax-mobile—WiMax mobile devices information. • wimax-fixed—WiMax fixed devices information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the information of all the interferers detected by a specified access point for the 802.11a network:

```
(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

To display access point channel utilization metrics, use the **show 802.11 cu-metrics** command.

show 802.11{**a** | **b**} **cu-metrics** *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show 802.11a cu-metrics** command:

```
(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

To display access point radio extended configurations, use the **show 802.11 extended** command.

show 802.11 {**a** | **b**} **extended**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
extended	Displays the 802.11a/b radio extended configurations.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The command output was expanded to include the Rx SOP threshold.

The following example shows how to display radio extended configurations:

```
(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
```

The following example shows how to display radio extended configurations and the Rx SOP threshold:

```
(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

To display the multicast-direct configuration state, use the **show 802.11 media-stream** command.

show 802.11 {**a** | **b** | **h**} **media-stream** *media_stream_name*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
h	Specifies the 802.11h network.
media_stream_name	Specified media stream name.

Command Default

None.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display the media-stream configuration:

```
> 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
```

Related Commands

show media-stream group summary

Show Commands: a to i

- show aaa auth, on page 1401
- show acl, on page 1402
- show acl detailed, on page 1404
- show acl url-acl detailed, on page 1405
- show acl summary, on page 1406
- show acl url-acl summary, on page 1407
- show advanced 802.11 channel, on page 1408
- show advanced 802.11 coverage, on page 1409
- show advanced 802.11 group, on page 1410
- show advanced hyperlocation summary, on page 1411
- show advanced hyperlocation ble-beacon, on page 1412
- show advanced 802.11 l2roam, on page 1413
- show advanced 802.11 logging, on page 1414
- show advanced 802.11 monitor, on page 1415
- show advanced 802.11 optimized roaming, on page 1416
- show advanced 802.11 profile, on page 1417
- show advanced 802.11 receiver, on page 1418
- show advanced 802.11 summary, on page 1419
- show advanced 802.11 txpower, on page 1420
- show advanced backup-controller, on page 1421
- show advanced dot11-padding, on page 1422
- show advanced hotspot, on page 1423
- show advanced max-1x-sessions, on page 1424
- show advanced probe, on page 1425
- show advanced rate, on page 1426
- show advanced timers, on page 1427
- show advanced client-handoff, on page 1428
- show advanced eap, on page 1429
- show advanced fra, on page 1430
- show advanced send-disassoc-on-handoff, on page 1432
- show advanced sip-preferred-call-no, on page 1433
- show advanced sip-snooping-ports, on page 1434
- show arp kernel, on page 1435

- show arp switch, on page 1436
- show ap auto-rf, on page 1437
- show ap aid-audit-mode, on page 1439
- show ap ccx rm, on page 1440
- show ap cdp, on page 1441
- show ap channel, on page 1443
- show ap config, on page 1444
- show ap config general , on page 1450
- show ap config global, on page 1452
- show ap core-dump, on page 1453
- show ap crash-file, on page 1454
- show ap data-plane, on page 1455
- show ap dtls-cipher-suite, on page 1456
- show ap ethernet tag, on page 1457
- show ap eventlog, on page 1458
- show ap flexconnect, on page 1459
- show ap image, on page 1460
- show ap image status, on page 1461
- show ap inventory, on page 1462
- show ap join stats detailed, on page 1463
- show ap join stats summary, on page 1464
- show ap join stats summary all, on page 1465
- show ap led-state, on page 1466
- show ap led-flash, on page 1467
- show ap link-encryption, on page 1468
- show ap max-count summary, on page 1469
- show ap monitor-mode summary, on page 1470
- show ap module summary, on page 1471
- show ap packet-dump status, on page 1472
- show ap prefer-mode stats, on page 1473
- show ap retransmit, on page 1474
- show ap stats, on page 1475
- show ap summary, on page 1478
- show ap tcp-mss-adjust, on page 1479
- show ap wlan, on page 1480
- show assisted-roaming , on page 1481
- show atf config, on page 1482
- show atf statistics ap, on page 1483
- show auth-list, on page 1484
- show avc applications, on page 1485
- show avc profile, on page 1486
- show avc statistics application, on page 1487
- show avc statistics client, on page 1489
- show avc statistics guest-lan, on page 1491
- show avc statistics remote-lan, on page 1492
- show avc statistics top-apps, on page 1493

- show avc statistics wlan, on page 1495
- show boot, on page 1497
- show band-select, on page 1498
- show buffers, on page 1499
- show cac voice stats, on page 1501
- show cac voice summary, on page 1502
- show cac video stats, on page 1503
- show cac video summary, on page 1505
- show call-control ap, on page 1506
- show call-control client, on page 1509
- show call-home summary, on page 1510
- show capwap reap association, on page 1511
- show capwap reap status, on page 1512
- show cdp, on page 1513
- show certificate compatibility, on page 1514
- show certificate lsc, on page 1515
- show certificate ssc, on page 1516
- show certificate summary, on page 1517
- show client ap, on page 1518
- show client calls, on page 1519
- show client ccx client-capability, on page 1520
- show client ccx frame-data, on page 1521
- show client ccx last-response-status, on page 1522
- show client ccx last-test-status, on page 1523
- show client ccx log-response, on page 1524
- show client ccx manufacturer-info, on page 1525
- show client ccx operating-parameters, on page 1526
- show client ccx profiles, on page 1527
- show client ccx results, on page 1529
- show client ccx rm, on page 1530
- show client ccx stats-report, on page 1532
- show client detail, on page 1533
- show client location-calibration summary, on page 1537
- show client probing, on page 1538
- show client roam-history, on page 1539
- show client summary, on page 1540
- show client summary guest-lan, on page 1542
- show client tsm, on page 1543
- show client username, on page 1545
- show client voice-diag, on page 1546
- show client wlan, on page 1547
- show cloud-services cmx summary, on page 1548
- show cloud-services cmx statistics, on page 1549
- show cts ap, on page 1550
- show cts environment-data, on page 1551
- show cts pacs, on page 1552

- show cts policy, on page 1553
- show cts sgacl, on page 1554
- show cts summary, on page 1555
- show cts sxp, on page 1556
- show coredump summary, on page 1557
- show country, on page 1558
- show country channels, on page 1559
- show country supported, on page 1560
- show cpu, on page 1562
- show custom-web, on page 1563
- show database summary, on page 1564
- show dhcp, on page 1565
- show dhcp proxy, on page 1566
- show dhcp timeout, on page 1567
- show dtls connections, on page 1568
- show exclusionlist, on page 1569
- show fabric summary, on page 1570
- show flexconnect acl detailed, on page 1572
- show flexconnect acl summary, on page 1573
- show flexconnect group detail, on page 1574
- show flexconnect group summary, on page 1575
- show flexconnect office-extend, on page 1576
- show flow exporter, on page 1577
- show flow monitor summary, on page 1578
- show guest-lan, on page 1579
- show icons summary, on page 1580
- show ike, on page 1581
- show interface summary, on page 1582
- show interface detailed, on page 1583
- show interface group, on page 1585
- show invalid-config, on page 1587
- show inventory, on page 1588
- show IPsec, on page 1589
- show ipv6 acl, on page 1591
- show ipv6 summary, on page 1592
- show guest-lan, on page 1593
- show icons file-info, on page 1594
- show ipv6 acl, on page 1595
- show ipv6 acl cpu, on page 1596
- show ipv6 acl detailed, on page 1597
- show ipv6 neighbor-binding, on page 1598
- show ipv6 ra-guard, on page 1602
- show ipv6 route summary, on page 1603
- show ipv6 summary, on page 1604
- show known ap, on page 1605

show aaa auth

To display the configuration settings for the AAA authentication server database, use the **show aaa auth** command.

show aaa auth

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the configuration settings for the AAA authentication server database:

```
(Cisco Controller) > show aaa auth
Management authentication server order:
    1..................................... local
    2..................................... tacacs
```

Related Commands

config aaa auth

config aaa auth mgmt

show acl

To display the access control lists (ACLs) that are configured on the controller, use the **show acl** command.

show acl { **cpu** | **detailed** *acl_name* | **summary** | **layer2** { **summary** | **detailed** *acl_name* } }

Syntax Description

cpu	Displays the ACLs configured on the controller's central processing unit (CPU).
detailed	Displays detailed information about a specific ACL.
acl_name	ACL name. The name can be up to 32 alphanumeric characters.
summary	Displays a summary of all ACLs configured on the controller.
layer2	Displays the Layer 2 ACLs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the access control lists on the CPU.

```
(Cisco Controller) >show acl cpu

CPU Acl Name.............................
Wireless Traffic.......................... Disabled
Wired Traffic............................. Disabled
Applied to NPU............................ No
```

The following example shows how to display a summary of the access control lists.

```
(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
```

The following example shows how to display the detailed information of the access control lists.

```
(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
```

Note The Counter field increments each time a packet matches an ACL rule, and the DenyCounter field increments each time a packet does not match any of the rules.

Related Commands

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

To display detailed DNS-based ACL information, use the **show acl detailed** command.

show acl detailed*acl_name*

Syntax Description

acl_name	Name of the access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.

The following is a sample output of the **show acl detailed** *acl_name* command.

```
(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 url-acl detailed

To display detailed URL ACL profile information, use the **show acl url-acl detailed** command.

show acl url-acl detailed *acl_name*

Syntax Description

acl_name	Name of the access control list.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows detailed information of a specific URL ACL profile:

```
(Cisco Controller) >show acl url-acl detailed
```

show acl summary

To display DNS-based ACL information, use the **show acl summary** command.

show aclsummary

Syntax Description

summary	Displays DNS-based ACL information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show acl summary** command.

```
(Cisco Controller) > show acl summary

 ACL Counter Status              Disabled
-------------------------------------
IPv4 ACL Name                    Applied
-------------------------------- -------
android                          No
StoreACL                         Yes
-------------------------------------
IPv6 ACL Name                    Applied
-------------------------------- -------                    1
```

show acl url-acl summary

To display a summary of the URL ACL profiles, use the **show acl url-acl summary** command.

show acl url-acl summary

Syntax Description

summary	Displays URL ACL profiles information.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows a summary of URL ACL profiles:

```
(Cisco Controller) > show acl summary

URL ACL Feature                 Disabled
ACL Counter Status               Enabled
-----------------------------------------
URL ACL Name       Applied
---------------    -------
test                 No
```

show advanced 802.11 channel

To display the automatic channel assignment configuration and statistics, use the **show advanced 802.11 channel** command.

show advanced 802.11{**a** | **b**} **channel**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the automatic channel assignment configuration and statistics:

```
(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

To display the configuration and statistics for coverage hole detection, use the **show advanced 802.11 coverage** command.

show advanced 802.11 {**a** | **b**} **coverage**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the statistics for coverage hole detection:

```
(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

To display 802.11a or 802.11b Cisco radio RF grouping, use the **show advanced 802.11 group** command.

show advanced 802.11{**a** | **b**} **group**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display Cisco radio RF group settings:

```
(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 hyperlocation summary

To view a summary of Cisco Hyperlocation configuration information, use the **show advanced hyperlocation summary** command.

show advanced hyperlocation summary

Command History

Release	Modification
8.1	This command was introduced in Release 8.1.

The following is a sample output:

```
(Cisco Controller) >show advanced hyperlocation summary

Hyperlocation..................................... DOWN
Hyperlocation NTP Server.......................... 0.0.0.0
Hyperlocation pak-rssi Threshold.................. -100
Hyperlocation pak-rssi Trigger-Threshold......... 10
Hyperlocation pak-rssi Reset-Threshold........... 8
Hyperlocation pak-rssi Timeout.................... 3

AP Name                          Ethernet MAC       Slots  Hyperlocation    Explicit AP
config
------------------------------  -----------------  -----  ---------------  ------------------
APA023.9FD8.EA4C                 40:ce:24:bf:8f:40  2      DOWN             0

APA023.9FD8.EA50                 40:ce:24:bf:8f:80  2      DOWN             0

APA023.9FD8.EA9C                 40:ce:24:bf:94:40  2      DOWN             0

AP0C75.BD13.B496                 a0:23:9f:8a:5c:00  2      DOWN             0
```

show advanced hyperlocation ble-beacon

To view information about BLE beacons in APs, use the **show advanced hyperlocation ble-beacon** command.

show advanced hyperlocation ble-beacon {**all** | **firmware-download summary** | **beacon-id** *id* | {**ap-name** *ap-name* | **ap-group** *group-name*}}

Syntax Description

all	Shows details of all BLE beacons.
firmware-download summary *value*	Lists all APs in BLE firmware download process.
beacon-id *id*	Shows information about the BLE beacon, the ID of which you specify.
ap-name *ap-name*	Shows information about the BLE beacon that is associated with the AP, the name of which you specify.
ap-group *group-name*	Shows information about the BLE beacon that is associated with the AP group, the name of which you specify.

Command History

Release	Modification
8.1	This command was introduced in Release 8.1.

The following is an example of how to view the BLE beacon information for all beacons:

```
(Cisco Controller) >show advanced hyperlocation ble-beacon all

Global Configuration

                    BLE Advertised Transmit Power: c5 (-59 dBm)

  BLE beacon ID                    UUID                        TX Power(dBm)     Interval(Hz)
    Status
-----------------    ----------------------------------------    --------------    ------------
    ----------
       1              00000000-0000-0000-0000-000000000000              0                 1
       Disabled

       2              00000000-0000-0000-0000-000000000000              0                 1
       Disabled

       3              00000000-0000-0000-0000-000000000000              0                 1
       Disabled

       4              00000000-0000-0000-0000-000000000000              0                 1
       Disabled

       5              00000000-0000-0000-0000-000000000000              0                 1
       Disabled
```

show advanced 802.11 l2roam

To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show advanced 802.11 l2roam** command.

show advanced 802.11 {**a** | **b**} **l2roam** {**rf-param** | **statistics**} *mac_address*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
rf-param	Specifies the Layer 2 frequency parameters.
statistics	Specifies the Layer 2 client roaming statistics.
mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show advanced 802.11b l2roam rf-param** command:

```
(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

To display 802.11a or 802.11b RF event and performance logging, use the **show advanced 802.11 logging** command.

show advanced 802.11{**a** | **b**} **logging**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display 802.11b RF event and performance logging:

```
(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

To display the 802.11a or 802.11b default Cisco radio monitoring, use the **show advanced 802.11 monitor** command.

show advanced 802.11{**a** | **b**} **monitor**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the radio monitoring for the 802.11b network:

```
(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

To display the optimized roaming configurations for 802.11a/b networks, use the **show advanced 802.11 optimized roaming** command.

show advanced 802.11 {**a** | **b**} **optimized roaming** [**stats**]

Syntax Description

stats	(Optional) Displays optimized roaming statistics for a 802.11a/b network.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to display the optimized roaming configurations for an 802.11a network:

```
(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
```

The following example shows how to display the optimized roaming statistics for an 802.11a network:

```
(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

To display the 802.11a or 802.11b lightweight access point performance profiles, use the **show advanced 802.11 profile** command.

show advanced 802.11{**a** | **b**} **profile** {**global** | *cisco_ap*}

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
global	Specifies all Cisco lightweight access points.
cisco_ap	Name of a specific Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the global configuration and statistics of an 802.11a profile:

```
(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
```

The following example shows how to display the configuration and statistics of a specific access point profile:

```
(Cisco Controller) >  show advanced 802.11 profile AP1
Cisco AP performance profile not customized
```

This response indicates that the performance profile for this lightweight access point is using the global defaults and has not been individually configured.

show advanced 802.11 receiver

To display the configuration and statistics of the 802.11a or 802.11b receiver, use the **show advanced 802.11 receiver** command.

show advanced 802.11{**a** | **b**} **receiver**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the configuration and statistics of the 802.11a network settings:

```
(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

To display the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary, use the **show advanced 802.11 summary** command.

show advanced 802.11{**a** | **b**} **summary**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the 802.11b access point settings:

```
(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(*)
```

Note An asterisk (*) next to a channel number or power level indicates that it is being controlled by the global algorithm settings.

show advanced 802.11 txpower

To display the 802.11a or 802.11b automatic transmit power assignment, use the **show advanced 802.11 txpower** command.

show advanced 802.11{**a** | **b**} **txpower**

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the configuration and statistics of the 802.11b transmit power cost:

```
(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

To display a list of primary and secondary backup controllers, use the **show advanced backup-controller** command.

show advanced backup-controller

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the backup controller information:

```
(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

To display the state of over-the-air frame padding on a wireless LAN controller, use the **show advanced dot11-padding** command.

show advanced dot11-padding

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to view the state of over-the-air frame padding:

```
(Cisco Controller) > show advanced dot11-padding
dot11-padding..................................... Disabled
```

show advanced hotspot

To display the advanced HotSpot parameters, use the **show advanced hotspot** command.

show advanced hotspot

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the advanced HotSpot parameters:

```
(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

To display the maximum number of simultaneous 802.1X sessions allowed per access point, use the **show advanced max-1x-sessions** command.

show advanced max-1x-sessions

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the maximum 802.1X sessions per access point:

```
(Cisco Controller) >show advanced max-1x-sessions
Max 802.1x session per AP at a given time........ 0
```

show advanced probe

To display the number of probes sent to the controller per access point per client and the probe interval in milliseconds, use the **show advanced probe** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the probe settings for the controller:

```
 (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

To display whether control path rate limiting is enabled or disabled, use the **show advanced rate** command.

show advanced rate

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the switch control path rate limiting mode:

```
(Cisco Controller) >show advanced rate
Control Path Rate Limiting.....................  Disabled
```

show advanced timers

To display the mobility anchor, authentication response, and rogue access point entry timers, use the **show advanced timers** command.

show advanced timers

Syntax Description

This command has no arguments or keywords.

Command Default

The defaults are shown in the “Examples” section.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the system timers setting:

```
(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

To display the number of automatic client handoffs after retries, use the **show advanced client-handoff** command.

show advanced client-handoff

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the client auto handoff mode after excessive retries:

```
(Cisco Controller) >show advanced client-handoff
Client auto handoff after retries.............  130
```

show advanced eap

To display Extensible Authentication Protocol (EAP) settings, use the **show advanced eap** command.

show advanced eap

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the EAP settings:

```
(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
```

Related Commands

config advanced eap

config advanced timers eap-identity-request-delay

config advanced timers eap-timeout

show advanced fra

To display Flexible Radio Assignment (FRA) settings, use the **show advanced fra** command.

show advanced fra

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.2	This command was introduced.

The following example shows the FRA settings when you set service-priority as coverage using the **config advanced fra service-priority coverage** command:

```
(Cisco Controller) > show advanced fra
FRA State..................................... Enabled
FRA Sensitivity............................... medium (95%)
FRA Interval.................................. 1 Hour(s)
  Last Run.................................... 2890 seconds ago
  Last Run Time............................... 0 seconds
Service Priority.............................. Coverage



AP Name                           MAC Address       Slot Current Band
COF %      Sensor %   Suggested Mode
------------------------------- ----------------- ---- --------------
---------- ---------- -------------------------
AP3800                            28:6f:7f:e0:60:40   0      2.4GHz
 None       None       (Static)

 COF : Coverage Overlap Factor
 []  : COF when radio was in 2.4GHz Band
```

The following example shows the FRA settings when you set service-priority as client-aware using the **config advanced fra service-priority client-aware** command:

```
 show advanced fra
FRA State..................................... Enabled
FRA Sensitivity............................... medium (95%)
FRA Interval.................................. 1 Hour(s)
  Last Run.................................... 3329 seconds ago
  Last Run Time............................... 0 seconds
Service Priority.............................. Client Aware
  Client Select Utilization Threshold......... 25%
  Client Reset Utilization Threshold.......... 5%
```

```
  802.11a Client Network Preference.............. default


AP Name                           MAC Address       Slot Current Band
COF %      Sensor %   Suggested Mode
-------------------------------- ----------------- ---- --------------
---------- ---------- -------------------------
AP3800                            28:6f:7f:e0:60:40   0     2.4GHz
  0          None       (Static)

 COF : Coverage Overlap Factor
 []  : COF when radio was in 2.4GHz Band
```

show advanced send-disassoc-on-handoff

To display whether the WLAN controller disassociates clients after a handoff, use the **show advanced send-disassoc-on-handoff** command.

show advanced send-disassoc-on-handoff

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show advanced send-disassoc-on-handoff** command:

```
(Cisco Controller) > show advanced send-disassoc-on-handoff
Send Disassociate on Handoff..................... Disabled
```

show advanced sip-preferred-call-no

To display the list of preferred call numbers, use the **show advanced sip-preferred-call-no** command.

show advanced sip-preferred-call-no

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show advanced sip-preferred-call-no** command:

```
(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

To display the port range for call snooping, use the **show advanced sip-snooping-ports** command.

show advanced sip-snooping-ports

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show advanced sip-snooping-ports** command:

```
(Cisco Controller) > show advanced sip-snooping-ports
 SIP Call Snoop Ports: 1000 - 2000
```

show arp kernel

To display the kernel Address Resolution Protocol (ARP) cache information, use the **show arp kernel** command.

show arp kernel

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show arp kernel** command:

```
(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

To display the Cisco wireless LAN controller MAC addresses, IP addresses, and port types, use the **show arp switch** command.

show arp switch

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show arp switch** command:

```
(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

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap auto-rf** command.

show ap auto-rf 802.11{**a** | **b**} *cisco_ap*

Syntax Description

a	Specifies the 802.11a network.
b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display auto-RF information for an access point:

```
(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

To view the AP aid-audit mode status, use the **show ap aid-audit mode** command.

show ap aid-audit mode

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.6	This command was introduced.

The following example shows how to display the aid-audit mode status:

```
(Cisco Controller) > show ap aid-audit-mode
 Aid Audit Mode ................................ Disabled
```

show ap ccx rm

To display an access point's Cisco Client eXtensions (CCX) radio management status information, use the **show ap ccx rm** command.

show ap ccx rm *ap_name* **status**

Syntax Description

ap_name	Specified access point name.
status	Displays the CCX radio management status information for an access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the status of the CCX radio management:

```
(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

To display the Cisco Discovery Protocol (CDP) information for an access point, use the **show ap cdp** command.

show ap cdp {**all** | **ap-name** *cisco_ap* | **neighbors** {**all** | **ap-name** *cisco_ap* | **detail** *cisco_ap*}}

Syntax Description

all	Displays the CDP status on all access points.
ap-name	Displays the CDP status for a specified access point.
cisco_ap	Specified access point name.
neighbors	Displays neighbors using CDP.
detail	Displays details about a specific access point neighbor using CDP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the CDP status of all access points:

```
(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
```

The following example shows how to display the CDP status of a specified access point:

```
(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
```

The following example shows how to display details about all neighbors using CDP:

```
(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
```

The following example shows how to display details about a specific neighbor with a specified access point using CDP:

```
(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
```

The following example shows how to display details about neighbors using CDP:

```
(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

To display the available channels for a specific mesh access point, use the **show ap channel** command.

show ap channel *ap_name*

Syntax Description

ap_name	Name of the mesh access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the available channels for a particular access point:

```
(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

To display the detailed configuration for a lightweight access point, use the **show ap config** command.

show ap config 802.11{**a** | **b**} [**summary**] *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a or 802.11b/g network.
802.11b	Specifies the 802.11b/g network.
summary	(Optional) Displays radio summary of all APs
cisco_ap	Lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed configuration for an access point:

```
(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
```

The following example shows how to display the detailed configuration for another access point:

```
(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
```

The following example shows how to display the general configuration of a Cisco access point:

```
(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

To display the access point specific syslog server settings for all access points, use the **show ap config general** command.

show ap config general *ap-name*

Syntax Description

ap-name	AP name

Command History

Release	Modification
8.0	This command was introduced
8.10.112.0	The output of the command is enhanced to show the status of AP antenna monitoring and failure detection for Cisco Wave 2 APs.

The following example shows how to display AP specific server settings:

```
(Cisco Controller) >show ap config general APc89c.1d53.6799
Cisco AP Identifier.............................. 76
Cisco AP Name.................................... APc89c.1d53.6799
Country code..................................... Multiple Countries:IN,JP,US
Regulatory Domain allowed by Country.............. 802.11bg:-AJPU 802.11a:-AJN
AP Country code.................................. US - United States
AP Regulatory Domain............................. 802.11bg:-A 802.11a:-A
Switch Port Number .............................. 1
MAC Address...................................... c8:9c:1d:53:67:99
IP Address Configuration......................... DHCP
IP Address....................................... 10.8.77.103
IP NetMask....................................... 255.255.255.0
Gateway IP Addr.................................. 10.8.77.1
NAT External IP Address.......................... None
CAPWAP Path MTU.................................. 1485
Telnet State..................................... Globally Disabled
Ssh State........................................ Globally Disabled
Cisco AP Location................................ default location
Cisco AP Floor Label............................. 0
Cisco AP Group Name.............................. apGroup2
Primary Cisco Switch Name.......................
Primary Cisco Switch IP Address.................. Not Configured
Secondary Cisco Switch Name.....................
Secondary Cisco Switch IP Address................ Not Configured
Tertiary Cisco Switch Name......................
Tertiary Cisco Switch IP Address.................. Not Configured
Administrative State ............................ ADMIN_ENABLED
Operation State ................................. REGISTERED
Mirroring Mode .................................. Disabled
AP Mode ......................................... Local
Public Safety ................................... Disabled
AP SubMode ...................................... Not Configured
Remote AP Debug ................................. Disabled
Logging trap severity level ..................... informational
Logging syslog facility ......................... system
S/W  Version .................................... 8.0.72.132
Boot  Version ................................... 12.4.23.0
Mini IOS Version ................................ 3.0.51.0
Stats Reporting Period .......................... 180
```

```
Stats Collection Mode ......................... normal
LED State...................................... Enabled
PoE Pre-Standard Switch........................ Disabled
PoE Power Injector MAC Addr.................... Disabled
Power Type/Mode................................ PoE/Full Power
Number Of Slots................................ 2
AP Model....................................... AIR-LAP1142N-A-K9
AP Image....................................... C1140-K9W8-M
IOS Version.................................... 15.3(20140302:180954)$
Reset Button................................... Enabled
AP Serial Number............................... FGL1510S3VZ
AP Certificate Type............................ Manufacture Installed
AP User Mode................................... AUTOMATIC
AP User Name................................... cisco
AP Dot1x User Mode............................. Not Configured
AP Dot1x User Name............................. Not Configured
Cisco AP system logging host................... 255.255.255.255
AP Up Time..................................... 0 days, 18 h 43 m 35 s
AP LWAPP Up Time............................... 0 days, 18 h 42 m 23 s
Join Date and Time............................. Wed Mar  5 07:26:07 2014
Join Taken Time................................ 0 days, 00 h 01 m 11 s
Memory Type.................................... DDR3
Memory Size.................................... 98294 KBytes
CPU Type....................................... PowerPC405ex CPU at 586Mhz, revision
number 0x147E
Flash Type..................................... Onboard Flash
Flash Size..................................... 31374 KBytes
GPS Present.................................... NO
Ethernet Vlan Tag.............................. Disabled
Ethernet Port Duplex........................... Auto
Ethernet Port Speed............................ Auto
AP Link Latency................................ Disabled
Rogue Detection................................ Enabled
AP TCP MSS Adjust.............................. Disabled
Hotspot Venue Group............................ Unspecified
Hotspot Venue Type............................. Unspecified
DNS server IP ........................... Not Available

AP broken antenna detection - Status ............ Enabled (Global)
RSSI Failure Threshold ......................... 40

--More-- or (q)uit
Weak RSSI ..................................... 60
Detection Time ................................ 12
If any broken antenna?......................... ALL
Memory Type.................................... DDR3
Memory Size.................................... 1028096 KBytes
CPU Type.....................................  ARMv7 Processor rev 1 (v7l)
```

show ap config global

To display the global syslog server settings for all access points that join the controller, use the **show ap config global** command.

show ap config global

Syntax Description

This command has no arguments and keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display global syslog server settings:

```
(Cisco Controller) >show ap config global
AP global system logging host.............................. 255.255.255.255
```

show ap core-dump

To display the memory core dump information for a lightweight access point, use the **show ap core-dump** command.

show ap core-dump *cisco_ap*

Syntax Description

cisco_ap	Cisco lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display memory core dump information:

```
(Cisco Controller) >show ap core-dump AP02
Memory core dump is disabled.
```

show ap crash-file

To display the list of both crash and radio core dump files generated by lightweight access points, use the **show ap crash-file** command.

show ap crash-file

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the crash file generated by the access point:

```
(Cisco Controller) >show ap crash-file
```

show ap data-plane

To display the data plane status for all access points or a specific access point, use the **show ap data-plane** command.

show ap data-plane {**all** | *cisco_ap*}

Syntax Description

all	Specifies all Cisco lightweight access points.
cisco_ap	Name of a Cisco lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the data plane status of all access points:

```
(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

To display the DTLS show cipher suite information, use the **show ap dtls-cipher-suite** command.

show ap dtls-cipher-suite

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to display DTLS cipher suite information:

```
(Cisco Controller) > show ap dtls-cipher-suite
DTLS Cipher Suite.............................. RSA-AES256-SHA
```

show ap ethernet tag

To display the VLAN tagging information of an Ethernet interface, use the **show ap ethernet tag** command.

show ap ethernet tag {**summary** | *cisco_ap*}

Syntax Description

summary	Displays the VLAN tagging information for all access points associated to the controller.
cisco_ap	Name of the Cisco lightweight access point. Displays the VLAN tagging information for a specific access point associated to the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If the access point is unable to route traffic or reach the controller using the specified trunk VLAN, it falls back to the untagged configuration. If the access point joins the controller using this fallback configuration, the controller sends a trap to a trap server such as the WCS, which indicates the failure of the trunk VLAN. In this scenario, the "Failover to untagged" message appears in show command output.

The following example shows how to display the VLAN tagging information for all access points associated to the controller:

```
(Cisco Controller) >show ap ethernet tag summary

AP Name              Vlan Tag Configuration
------------------   -------
AP2                  7  (Failover to untagged)
charan.AP1140.II     disabled
```

show ap eventlog

To display the contents of the event log file for an access point that is joined to the controller, use the **show ap eventlog** command.

show ap eventlog *ap_name*

Syntax Description

ap_name	Event log for the specified access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the event log of an access point:

```
(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

To view the details of APs in FlexConnect mode, use the **show ap flexconnect** command.

show ap flexconnect module-vlan *ap-name*

Syntax Description

module-vlan	Displays the status of FlexConnect local switching and VLAN ID value
ap-name	Cisco AP name

Command History

Release	Modification
8.1	This command was introduced

show ap image

To display the detailed information about the predownloaded image for specified access points, use the **show ap image** command.

show ap image {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Name of the lightweight access point.
all	Specifies all access points.

Note If you have an AP that has the name *all*, it conflicts with the keyword **all** that specifies all access points. In this scenario, the keyword **all** takes precedence over the AP that is named *all*.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

show ap image status

To view download status on all APs, use the **show ap image status** command.

show ap image status

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
8.2	This command was introduced.

show ap inventory

To display inventory information for an access point, use the **show ap inventory** command.

show ap inventory {*ap-name* | **all**}

Syntax Description

ap-name	Inventory for the specified AP.
all	Inventory for all the APs.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the inventory of an access point:

```
(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

To display all join-related statistics collected for a specific access point, use the **show ap join stats detailed** command.

show ap join stats detailed *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display join information for a specific access point trying to join the controller:

```
(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

To display the last join error detail for a specific access point, use the **show ap join stats summary** command.

show ap join stats summary *ap_mac*

Syntax Description

ap_mac	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To obtain the MAC address of the 802.11 radio interface, enter the **show interface** command on the access point.

The following example shows how to display specific join information for an access point:

```
(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

To display the MAC addresses of all the access points that are joined to the controller or that have tried to join, use the **show ap join stats summary all** command.

show ap join stats summary all

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of join information for all access points:

```
(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

To view the LED state of all access points or a specific access point, use the **show ap led-state** command.

show ap led-state {**all** | *cisco_ap*}

Syntax Description

all	Shows the LED state for all access points.
cisco_ap	Name of the access point whose LED state is to be shown.

Command Default

The AP LED state is enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to get the LED state of all access points:

```
(Cisco Controller) >show ap led-state all
Global LED State: Enabled (default)
```

show ap led-flash

To display the LED flash status of an access point, use the **show ap led-flash** command.

show ap led-flash *cisco_ap*

Syntax Description

cisco_ap	Enter the name of the Cisco AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the LED flash status of an access point:

```
(Cisco Controller) >show ap led-flash
```

show ap link-encryption

To display the MAC addresses of all the access points that are joined to the controller or that have tried to join, use the **show ap link-encryption** command.

show ap link-encryption {**all** | *cisco_ap*}

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the lightweight access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the link encryption status of all access points:

```
(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

To display the maximum number of access points supported by the controller, use the **show ap max-count summary**command.

show ap max-count summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show ap max-count summary**command:

```
(Cisco Controller) >show ap max-count

The max number of AP's supported.................. 500
```

show ap monitor-mode summary

To display the current channel-optimized monitor mode settings, use the **show ap monitor-mode summary** command.

show ap monitor-mode summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display current channel-optimized monitor mode settings:

```
(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

To view detailed information about the external module, for a specific Cisco AP or for all Cisco APs, use the **show ap module summary** command.

show ap module summary {*ap-name* | **all**}

Syntax Description

ap-name	Cisco AP name that has the external module
all	All Cisco APs that have the external module

Command History

Release	Modification
8.1	This command was introduced.

show ap packet-dump status

To display access point Packet Capture configurations, use the **show ap packet-dump status** command.

show ap packet-dump status

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Packet Capture does not work during intercontroller roaming.

The controller does not capture packets created in the radio firmware and sent out of the access point, such as the beacon or probe response. Only packets that flow through the Radio driver in the Tx path are captured.

The following example shows how to display the access point Packet Capture configurations:

```
(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

To view prefer-mode global and per AP group statistics, use the **show ap prefer-mode stats** command.

show ap prefer-mode stats

Syntax Description

stats	Displays prefer-mode global and per AP group statistics

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

show ap retransmit

To display access point control packet retransmission parameters, use the**show ap retransmit** command.

show ap retransmit {**all** | *cisco_ap*}

Syntax Description

all	Specifies all access points.
cisco_ap	Name of the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the control packet retransmission parameters of all access points on a network:

```
(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

To display the statistics for a Cisco lightweight access point, use the **show ap stats** command.

show ap stats {**802.11**{**a** | **b**} | **wlan** | **ethernet summary**} *cisco_ap* [**tsm** {*client_mac* | **all**}]

Syntax Description

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
wlan	Specifies WLAN statistics.
ethernet	Specifies AP ethernet interface statistics.
summary	Displays ethernet interface summary of all the connected Cisco access points.
cisco_ap	Name of the lightweight access point.
tsm	(Optional) Specifies the traffic stream metrics.
client_mac	(Optional) MAC address of the client.
all	(Optional) Specifies all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command was modified. The OEAP WMM Counters were added to the output.

The following example shows how to display statistics of an access point for the 802.11b network:

```
(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

To display a summary of all lightweight access points attached to the controller, use the **show ap summary** command.

show ap summary [*cisco_ap*]

Syntax Description

cisco_ap	(Optional) Type sequence of characters that make up the name of a specific AP or a group of APs, or enter a wild character search pattern.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

A list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the controller port number appears. When you specify

The following example shows how to display a summary of all connected access points:

```
(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

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap tcp-mss-adjust** command.

show ap tcp-mss-adjust {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Specified lightweight access point name.
all	Specifies all access points.

Note If an AP itself is configured with the keyword **all**, the all access points case takes precedence over the AP that is with the keyword **all**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display Transmission Control Protocol (TCP) maximum segment size (MSS) information of all access points:

```
(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

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point, use the **show ap wlan** command.

show ap wlan 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
ap_name	Lightweight access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display BSSIDs of an access point for the 802.11b network:

```
(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

To display assisted roaming and 802.11k configurations, use the **show assisted-roaming** command.

show assisted-roaming

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display assisted roaming and 802.11k configurations:

```
(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
```

Related Commands

config assisted-roaming

config wlan assisted-roaming

debug 11k

show atf config

To monitor Cisco Airtime Fairness configuration, use the **show atf config** command.

show atf config {**all** | {**ap-name***ap-name*} | {**802.11**{**a** | **b**}} | **policy** | **wlan**}

Syntax Description

all	Shows Cisco ATF configuration of all radios
ap-name	Shows Cisco ATF configuration of an AP
ap-name	AP name that you must specify
802.11a	Shows Cisco ATF configuration of all 5-GHz radios
802.11b	Shows Cisco ATF configuration of all 2.4-GHz radios
policy	Shows configuration of all airtime policies
wlan	Shows Cisco ATF configuration of all WLANs

Command Default

None

Command History

Release	Modification
8.1	This command was introduced

This example shows how to monitor Cisco Airtime Fairness configuration:

```
(Cisco Controller) >show atf config all
```

show atf statistics ap

To monitor Cisco Airtime Fairness statistics, use the **show atf statistics** command.

show atf statistics ap *ap-name* **802.11**{**a** | **b**} {**summary** | *wlan-id* | *policy-id*}

Syntax Description

802.11a	Shows detailed statistics on all 5-GHz radios.
802.11b	Shows detailed statistics on all 2.4-GHz radios.
summary	Shows summary statistics for the AP.
wlan *wlan-id*	Shows detailed ATF statistics for the specified WLAN.
policy *policy-name*	Shows detailed ATF statistics for the specified policy name.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

This example shows how to monitor Cisco Airtime Fairness statistics:

```
(Cisco Controller) >show atf statistics ap Ap01323 802.11a summary
```

show auth-list

To display the access point authorization list, use the **show auth-list** command.

show auth-list

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the access point authorization list:

```
(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

To display all the supported Application Visibility and Control (AVC) applications, use the **show avc applications** command.

show avc applications

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

Usage Guidelines

AVC uses the Network-Based Application Recognition (NBAR) deep packet inspection technology to classify applications based on the protocol they use. Using AVC, the controller can detect more than 1500 Layer 4 to Layer 7 protocols.

The following is a sample output of the **show avc applications** command:

```
(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 profile

To display Application Visibility and Control (AVC) profiles, use the **show avc profile** command.

show avc profile {**summary** | **detailed** *profile_name* }

Syntax Description

summary	Displays a summary of AVC profiles.
detailed	Displays the details of an AVC profile.
profile_name	Name of the AVC profile. The profile name can be up to 32 case-sensitive, alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc profile summary** command.

```
(Cisco Controller) > show avc profile summary

 Profile-Name                      Number of Rules
  ============                      ==============
  profile 1                                3
  avc_profile2                             1
```

The following is a sample output of the **show avc profile detailed** command.

```
(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 statistics application

To display the statistics of an application, use the **show avc statistics application** command.

show avc statistics application *application_name* **top-users** [**downstream wlan** | **upstream wlan** | **wlan**] [*wlan_id*] }

Syntax Description

application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-users	Displays AVC statistics for top application users.
downstream	(Optional) Displays statistics of top downstream applications.
wlan	(Optional) Displays AVC statistics of a WLAN.
wlan_id	WLAN identifier from 1 to 512.
upstream	(Optional) Displays statistics of top upstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics application** command:

```
(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

To display the client Application Visibility and Control (AVC) statistics, use the **show avc statistics client** command.

show avc statistics client *client_MAC* {**application** *application_name* | **top-apps** [**upstream** | **downstream**] }

Syntax Description

client_MAC	MAC address of the client.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-apps	Displays AVC statistics for top applications.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics client** command:

```
(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
```

The following is a sample output of the **show avc statistics client** command.

```
(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

To display the Application Visibility and Control (AVC) statistics of a guest LAN, use the **show avc statistics guest-lan** command.

show avc statistics guest-lan *guest-lan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

guest-lan_id	Guest LAN identifier from 1 to 5.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics** command.

```
(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

To display the Application Visibility and Control (AVC) statistics of a remote LAN, use the **show avc statistics remote-lan** command.

show avc statistics remote-lan *remote-lan_id* { **application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**] }

Syntax Description

remote-lan_id	Remote LAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics remote-lan** command.

```
(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

To display the Application Visibility and Control (AVC) statistics for the most used applications, use the **show avc statistics top-apps** command.

show avc statistics top-apps [**upstream** | **downstream**]

Syntax Description

upstream	(Optional) Displays statistics of the most used upstream applications.
downstream	(Optional) Displays statistics of the most used downstream applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics top-aps** command:

```
(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
```

Related Commands

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

To display the Application Visibility and Control (AVC) statistics of a WLAN, use the **show avc statistics wlan** command.

show avc statistics wlan *wlan_id* {**application** *application_name* | **top-app-groups** [**upstream** | **downstream**] | **top-apps** [**upstream** | **downstream**]}

Syntax Description

wlan_id	WLAN identifier from 1 to 512.
application	Displays AVC statistics for an application.
application_name	Name of the application. The application name can be up to 32 case-sensitive, alphanumeric characters.
top-app-groups	Displays AVC statistics for top application groups.
upstream	(Optional) Displays statistics of top upstream applications.
downstream	(Optional) Displays statistics of top downstream applications.
top-apps	Displays AVC statistics for top applications.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

The following is a sample output of the **show avc statistics** command.

```
(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
```

The following is a sample output of the **show avc statistics wlan** command.

```
(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

To display the primary and backup software build numbers with an indication of which is active, use the **show boot** command.

show boot

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Each Cisco wireless LAN controller retains one primary and one backup operating system software load in nonvolatile RAM to allow controllers to boot off the primary load (default) or revert to the backup load when desired.

The following is a sample output of the **show boot** command:

```
(Cisco Controller) > show boot
Primary Boot Image.............................. 3.2.13.0 (active)
Backup Boot Image............................... 3.2.15.0
```

Related Commands

config boot

show band-select

To display band selection information, use the **show band-select** command.

show band-select

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show band-select** command:

```
(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
```

Related Commands

config band-select

config wlan band-select

show buffers

To display buffer information of the controller, use the **show buffers** command.

show buffers

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show buffers** command:

```
(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

To view the detailed voice CAC statistics of the 802.11a or 802.11b radio, use the **show cac voice stats** command.

show cac voice stats {**802.11a** | **802.11b**}

Syntax Description

802.11a	Displays detailed voice CAC statistics for 802.11a.
802.11b	Displays detailed voice CAC statistics for 802.11b/g.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cac voice stats 802.11b** command:

```
(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

To view the list of all APs with brief voice statistics (includes bandwidth used, maximum bandwidth available, and the number of calls information), use the **show cac voice summary** command.

show cac voice summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cac voice summary** command:

```
(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

To view the detailed video CAC statistics of the 802.11a or 802.11b radio, use the **show cac video stats** command.

show cac video stats {**802.11a** | **802.11b**}

Syntax Description

802.11a	Displays detailed video CAC statistics for 802.11a.
802.11b	Displays detailed video CAC statistics for 802.11b/g.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cac video stats 802.11b** command:

```
(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
```

Related Commands

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

To view the list of all access points with brief video statistics (includes bandwidth used, maximum bandwidth available, and the number of calls information), use the **show cac video summary** command.

show cac video summary

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cac video summary** command:

```
(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
```

Related Commands

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

Note The **show call-control ap** command is applicable only for SIP based calls.

To see the metrics for successful calls or the traps generated for failed calls, use the **show call-control ap** command.

show call-control ap {**802.11a** | **802.11b**} *cisco_ap* {**metrics** | **traps**}

Syntax Description

802.11a	Specifies the 802.11a network
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco access point name.
metrics	Specifies the call metrics information.
traps	Specifies the trap information for call control.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To aid in troubleshooting, the output of this command shows an error code for any failed calls. This table explains the possible error codes for failed calls.

Table 12: Error Codes for Failed VoIP Calls

Error Code	Integer	Description
1	unknown	Unknown error.
400	badRequest	The request could not be understood because of malformed syntax.
401	unauthorized	The request requires user authentication.
402	paymentRequired	Reserved for future use.
403	forbidden	The server understood the request but refuses to fulfill it.
404	notFound	The server has information that the user does not exist at the domain specified in the Request-URI.
405	methodNotallowed	The method specified in the Request-Line is understood but not allowed for the address identified by the Request-URI.

Error Code	Integer	Description
406	notAcceptable	The resource identified by the request is only capable of generating response entities with content characteristics that are not acceptable according to the Accept header field sent in the request.
407	proxyAuthenticationRequired	The client must first authenticate with the proxy.
408	requestTimeout	The server could not produce a response within a suitable amount of time.
409	conflict	The request could not be completed due to a conflict with the current state of the resource.
410	gone	The requested resource is no longer available at the server, and no forwarding address is known.
411	lengthRequired	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
413	requestEntityTooLarge	The server is refusing to process a request because the request entity-body is larger than the server is willing or able to process.
414	requestURITooLarge	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415	unsupportedMediaType	The server is refusing to service the request because the message body of the request is in a format not supported by the server for the requested method.
420	badExtension	The server did not understand the protocol extension specified in a Proxy-Require or Require header field.
480	temporarilyNotAvailable	The callee's end system was contacted successfully, but the callee is currently unavailable.
481	callLegDoesNotExist	The UAS received a request that does not match any existing dialog or transaction.
482	loopDetected	The server has detected a loop.
483	tooManyHops	The server received a request that contains a Max-Forwards header field with the value zero.
484	addressIncomplete	The server received a request with a Request-URI that was incomplete.
485	ambiguous	The Request-URI was ambiguous.
486	busy	The callee's end system was contacted successfully, but the callee is currently not willing or able to take additional calls at this end system.

Error Code	Integer	Description
500	internalServerError	The server encountered an unexpected condition that prevented it from fulfilling the request.
501	notImplemented	The server does not support the functionality required to fulfill the request.
502	badGateway	The server, while acting as a gateway or proxy, received an invalid response from the downstream server it accessed in attempting to fulfill the request.
503	serviceUnavailable	The server is temporarily unable to process the request because of a temporary overloading or maintenance of the server.
504	serverTimeout	The server did not receive a timely response from an external server it accessed in attempting to process the request.
505	versionNotSupported	The server does not support or refuses to support the SIP protocol version that was used in the request.
600	busyEverywhere	The callee's end system was contacted successfully, but the callee is busy or does not want to take the call at this time.
603	decline	The callee's machine was contacted successfully, but the user does not want to or cannot participate.
604	doesNotExistAnywhere	The server has information that the user indicated in the Request-URI does not exist anywhere.
606	notAcceptable	The user's agent was contacted successfully, but some aspects of the session description (such as the requested media, bandwidth, or addressing style) were not acceptable.

The following is a sample output of the **show call-controller ap** command that displays successful calls generated for an access point:

```
(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
```

The following is a sample output of the **show call-control ap** command that displays metrics of traps generated for an AP.

```
(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

To see call information for a call-aware client when Voice-over-IP (VoIP) snooping is enabled and the call is active, use the **show call-control client** command

show call-control client callInfo *client_MAC_address*

Syntax Description

callInfo	Specifies the call-control information.
client_MAC_address	Client MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example is a sample output of the **show call-controller client** command:

```
(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

To view the Call Home details, use the **show call-home summary** command.

show call-home summary

Command History

Release	Modification
8.2	This command was introduced.

The following example shows the call-home summary:

```
(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

To display the list of clients associated with an access point and their SSIDs, use the **show capwap reap association** command.

show capwap reap association

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display clients associated to an access point and their SSIDs:

```
(Cisco Controller) >show capwap reap association
```

show capwap reap status

To display the status of the FlexConnect access point (connected or standalone), use the **show capwap reap status** command.

show capwap reap status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The command shows only the VLAN when configured as AP-specific.

The following example shows how to display the status of the FlexConnect access point:

```
(Cisco Controller) >show capwap reap status
```

show cdp

To display the status and details of the Cisco Discovery Protocol (CDP), use the **show cdp** command.

show cdp {**neighbors** [**detail**] | **entry all** | **traffic**}

Syntax Description

neighbors	Displays a list of all CDP neighbors on all interfaces.
detail	(Optional) Displays detailed information of the controller's CDP neighbors. This command shows only the CDP neighbors of the controller; it does not show the CDP neighbors of the controller's associated access points.
entry all	Displays all CDP entries in the database.
traffic	Displays CDP traffic information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cdp** command:

```
(Cisco Controller) > show cdp
CDP counters :
Total packets output: 0, Input: 0
Chksum error: 0
No memory: 0, Invalid packet: 0,
```

Related Commands

config cdp

config ap cdp

show ap cdp

show certificate compatibility

To display whether or not certificates are verified as compatible in the Cisco wireless LAN controller, use the **show certificate compatibility** command.

show certificate compatibility

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show certificate compatibility** command:

```
(Cisco Controller) > show certificate compatibility
Certificate compatibility mode:.............. off
```

show certificate lsc

To verify that the controller has generated a Locally Significant Certificate (LSC), use the **show certificate lsc summary** command.

show certificate lsc {**summary** | **ap-provision**}

Syntax Description

summary	Displays a summary of LSC certificate settings and certificates.
ap-provision	Displays details about the access points that are provisioned using the LSC.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show certificate lsc summary** command:

```
(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
```

This example shows how to display the details about the access points that are provisioned using the LSC:

```
(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

To view the Self Signed Device Certificate (SSC) and hash key of the virtual controller, use the **show certificate ssc** command.

show certificate ssc

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show certificate ssc** command :

```
(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

To verify that the controller has generated a certificate, use the **show certificate summary** command.

show certificate summary

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show certificate summary** command:

```
(Cisco Controller) > show certificate summary
Web Administration Certificate..................... Locally Generated
Web Authentication Certificate..................... Locally Generated
Certificate compatibility mode:.................... off
```

show client ap

To display the clients on a Cisco lightweight access point, use the **show client ap** command.

show client ap 802.11{**a** | **b**} *cisco_ap*

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11b/g network.
cisco_ap	Cisco lightweight access point name.

Command Default

None

Usage Guidelines

The **show client ap** command may list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the exclusion list.

This example shows how to display client information on an access point:

```
(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

To display the total number of active or rejected calls on the controller, use the **show client calls** command.

show client calls {**active** | **rejected**} {**802.11a** | **802.11bg** | **all**}

Syntax Description

active	Specifies active calls.
rejected	Specifies rejected calls.
802.11a	Specifies the 802.11a network.
802.11bg	Specifies the 802.11b/g network.
all	Specifies both the 802.11a and 802.11b/g network.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client calls active 802.11a** command :

```
(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

To display the client's capability information, use the **show client ccx client-capability** command.

show client ccx client-capability *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command displays the client's available capabilities, not the current settings for the capabilities.

The following is a sample output of the **show client ccx client-capability** command:

```
(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

To display the data frames sent from the client for the last test, use the **show client ccx frame-data** command.

show client ccx frame-data *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx frame-data** command:

```
(Cisco Controller) >show client ccx frame-data
 xx:xx:xx:xx:xx:xx
```

show client ccx last-response-status

To display the status of the last test response, use the **show client ccx last-response-status** command.

show client ccx last-response-status *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx last-response-status** command:

```
(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

To display the status of the last test, use the **show client ccx last-test-status** command.

show client ccx last-test-status *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx last-test-status** command:

```
(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

To display a log response, use the **show client ccx log-response** command.

show client ccx log-response {**roam** | **rsna** | **syslog**} *client_mac_address*

Syntax Description

roam	(Optional) Displays the CCX client roaming log response.
rsna	(Optional) Displays the CCX client RSNA log response.
syslog	(Optional) Displays the CCX client system log response.
client_mac_address	Inventory for the specified access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx log-response syslog** command:

```
(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'
```

The following example shows how to display the client roaming log response:

```
(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

To display the client manufacturing information, use the **show client ccx manufacturer-info** command.

show client ccx manufacturer-info *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx manufacturer-info** command:

```
(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

To display the client operating-parameters, use the **show client ccx operating-parameters** command.

show client ccx operating-parameters *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx operating-parameters** command:

```
(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

To display the client profiles, use the **show client ccx profiles** command.

show client ccx profiles *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx profiles** command:

```
(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

To display the results from the last successful diagnostic test, use the **show client ccx results** command.

show client ccx results *client_mac_address*

Syntax Description

client_mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx results** command:

```
(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

To display Cisco Client eXtension (CCX) client radio management report information, use the **show client ccx rm** command.

show client ccx rm *client_MAC* {**status** | {**report** {**chan-load** | **noise-hist** | **frame** | **beacon** | **pathloss**} } }

Syntax Description

client_MAC	Client MAC address.
status	Displays the client CCX radio management status information.
report	Displays the client CCX radio management report.
chan-load	Displays radio management channel load reports.
noise-hist	Displays radio management noise histogram reports.
beacon	Displays radio management beacon load reports.
frame	Displays radio management frame reports.
pathloss	Displays radio management path loss reports.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the client radio management status information:

```
(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
```

The following example shows how to display the client radio management load reports:

```
(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
```

The following example shows how to display the client radio management noise histogram reports:

```
(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

To display the Cisco Client eXtensions (CCX) statistics report from a specified client device, use the **show client ccx stats-report** command.

show client ccx stats-report *client_mac_address*

Syntax Description

client_mac_address	Client MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client ccx stats-report** command:

```
(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

To display IP addresses per client learned through DNS snooping (DNS-based ACL), use the **show client detail** *mac_address* command.

show client detail *mac_address*

Syntax Description

mac_address	MAC address of the client.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced.

The following is a sample output of the **show client detail** *mac_address* command.

```
(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

To display client location calibration summary information, use the **show client location-calibration summary** command.

show client location-calibration summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the location calibration summary information:

```
(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

To display the number of probing clients, use the **show client probing** command.

show client probing

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the number of probing clients:

```
(Cisco Controller) >show client probing
Number of Probing Clients..................... 0
```

show client roam-history

To display the roaming history of a specified client, use the **show client roam-history** command.

show client roam-history *mac_address*

Syntax Description

mac_address	Client MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command provides the following information:

- The time when the report was received
- The MAC address of the access point to which the client is currently associated
- The MAC address of the access point to which the client was previously associated
- The channel of the access point to which the client was previously associated
- The SSID of the access point to which the client was previously associated
- The time when the client disassociated from the previous access point
- The reason for the client roam

Note For non-CCXv4 clients, the Layer 2 roam reason is not displayed in the command output. For more information, see CSCvv85022.

Examples

The following is a sample output of the **show client roam-history** command:

```
(Cisco Controller) > show client roam-history 00:14:6c:0a:57:77
```

show client summary

To display a summary of clients associated with a Cisco lightweight access point, use the **show client summary** command.

show client summary [*ssid / ip / username / devicetype*]

Syntax Description

This command has no arguments or keywords.

Syntax Description

ssid / ip / username / devicetype	(Optional) Displays active clients selective details on any of the following parameters or all the parameters in any order: • SSID • IP addresss • Username • Device type (such as Samsung-Device or WindowsXP-Workstation)

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Use **show client ap** command to list the status of automatically disabled clients. Use the **show exclusionlist** command to display clients on the exclusion list.

The following example shows how to display a summary of the active clients:

```
(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
```

The following example shows how to display all clients that are WindowsXP-Workstation device type:

```
(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

To display the active wired guest LAN clients, use the **show client summary guest-lan** command.

show client summary guest-lan

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client summary guest-lan** command:

```
(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
```

Related Commands

show client summary

show client tsm

To display the client traffic stream metrics (TSM) statistics, use the **show client tsm** command.

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

Syntax Description

802.11a	Specifies the 802.11a network.
802.11b	Specifies the 802.11 b/g network.
client_mac	MAC address of the client.
ap_mac	MAC address of the tsm access point.
all	Specifies the list of all access points to which the client has associations.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client tsm 802.11a** command:

```
(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
```

Related Commands

show client ap

show client detail

show client summary

show client username

To display the client data by the username, use the **show client username** command.

show client username *username*

Syntax Description

username	Client's username. You can view a list of the first eight clients that are in RUN state associated to controller's access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client username** command:

```
(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

To display voice diagnostics statistics, use the **show client voice-diag** command.

show client voice-diag {**quos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

quos-map	Displays information about the QoS/DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history	Displays information about history of the last three roamings. The output contains the timestamp, access point associated with the roaming, the roaming reason, and if there is a roaming failure, the reason for the roaming failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays the status of voice diagnostics for clients.
tspec	Displays TSPEC for the voice diagnostic for clients.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show client voice-diag status** command:

```
(Cisco Controller) > show client voice-diag status
Voice Diagnostics Status: FALSE
```

Related Commands

show client ap

show client detail

show client summary

debug voice-diag

show client wlan

To display the summary of clients associated with a WLAN, use the **show client wlan** command.

show client wlan *wlan_id* [**devicetype** *device*]

Syntax Description

wlan_id	Wireless LAN identifier from 1 to 512.
devicetype	(Optional) Displays all clients with the specified device type.
device	Device type. For example, Samsung-Device or WindowsXP-Workstation.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following are sample outputs of the **show client wlan** command:

```
(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

To view the cmx cloud services summary, use the **show cloud-services cmx summary** command.

show cloud-services cmx summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows the CMX Cloud Services summary:

```
(Cisco Controller) >show cloud-services cmx summary
```

show cloud-services cmx statistics

To view the cmx cloud services statistics, use the **show cloud-services cmx statistics** command.

show cloud-services cmx statistics

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows the CMX Cloud Services statistics:

```
(Cisco Controller) >show cloud-services cmx statistics
```

show cts ap

To view CTS AP SGT information, use the **show cts ap** command.

show cts ap {**sgt-info** *cisco-ap* | **summary**}

Syntax Description

sgt-info *cisco-ap*	Shows CTS SGT information for a specific AP
summary	Shows CTS SGT information for all APs.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

This example shows how to view CTS SGT information for all APs:

```
(Cisco Controller) >show cts ap summary

Inline Tag Status.............................. Disabled
SGACL enforcement.............................. Disabled
SXP State...................................... Enabled
Default Password............................... ****
Listener hold-time min ........................ 2
Listener hold-time max ........................ 3
Speaker hold-time ............................. 120
Reconciliation time period..................... 120
Retry time period ............................. 120
Total num of SXP Connections................... 0
   Peer IP            Password         Mode
---------------     ------------      ------
```

show cts environment-data

To view CTS Environment data, use the **show cts environment-data** command.

show cts environment-data

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

```
(Cisco Controller) >show cts environment-data

CTS Environment Data
====================

Current State.................................. START
Last status.................................... WAITING_RESPONSE

Environment data is empty
```

show cts pacs

To view CTS Protected Access Credential (PAC) provisioning information, use the **show cts pacs** command.

show cts pacs

Command Default None

Command History

Release	Modification
8.4	This command was introduced.

show cts policy

To view CTS SGT policy information, use the **show cts policy** command.

show cts policy {**all** | *sgt-tag*}

Syntax Description

all	Shows all SGT policy information
sgt-tag	Shows policy information of a specific SGT

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

This example shows how to view all SGT policy information:

```
(Cisco Controller) >show cts policy all

Policy Matrix for SGT..... Unknown-0
  Generation Id..... 0x0
  Policy Download Status.....  Failed
  Number of clients with this SGT..... 0


Policy Matrix for SGT..... Default-65535
  Generation Id..... 0x0
  Policy Download Status.....  Failed
  Number of clients with this SGT..... 0
```

show cts sgacl

To view CTS SGACL information, use the **show cts sgacl** command.

show cts sgacl {**all** | *sgacl-name*}

Syntax Description

all	Shows all SGACL information
sgt-tag	Shows information for a specific SGACL

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

show cts summary

To view CTS summary, use the **show cts summary** command.

show cts summary

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

```
(Cisco Controller) >show cts summary

 CTS Status..................................... Enabled
 CTS Device Identity............................ Not Configured
 Inline Tag Status.............................. Disabled
```

show cts sxp

To view CTS SXP information, use the **show cts sxp** command.

show cts sxp { { **ap** { **connections** | **summary** } *cisco-ap* } | **connections** | **summary** }

Command Default None

Command History

Release	Modification
8.4	This command was introduced.

show coredump summary

To display a summary of the controller's core dump file, use the **show coredump summary** command.

show coredump summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show coredump summary** command:

```
(Cisco Controller) > show coredump summary
Core Dump is enabled
FTP Server IP..................................... 10.10.10.17
FTP Filename...................................... file1
FTP Username...................................... ftpuser
FTP Password...................................... *********
```

Related Commands

config coredump

config coredump ftp

config coredump username

show country

To display the configured country and the radio types that are supported, use the **show country** command.

show country

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the configured countries and supported radio types:

```
(Cisco Controller) >show country
Configured Country..............................  United States
Configured Country Codes
US  - United States.............................  802.11a / 802.11b / 802.11g
```

show country channels

To display the radio channels supported in the configured country, use the **show country channels** command.

show country channels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the auto-RF channels for the configured countries:

```
(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

To display a list of the supported country options, use the **show country supported** command.

show country supported

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a list of all the supported countries:

```
(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

To display current WLAN controller CPU usage information, use the **show cpu** command.

show cpu

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show cpu** command:

```
(Cisco Controller) > show cpu
Current CPU load: 2.50%
```

show custom-web

To display all the web authentication customization information, use the **show custom-web** command.

show custom-web *all remote-lan guest-lan sleep-client webauth-bundle wlan*

Syntax Description

all	Display all Web-Auth customization information.
remote-lan	Display per WLAN Web-Auth customization information.
guest-lan	Display per Guest LAN Web-Auth customization information.
sleep-client	Display all Web-Auth Sleeping Client entries summary.
webauth-bundle	Display the content of Web-Auth Bundle.
wlan	Display per WLAN Web-Auth customization information.

Command History

Release	Modification
7.6	This command was introduced in the release earlier than 7.6.
8.2	This command was modified and the all, remote-lan, guest-lan, sleep-client, webauth-bundle, and wlan keywords are added.

The following is a sample output of the **show custom-web all** command:

```
(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

To display the maximum number of entries in the database, use the **show database summary** command.

show database summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

The following is a sample output of the **show database summary** command:

```
(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
```

Related Commands

config database size

show dhcp

To display the internal Dynamic Host Configuration Protocol (DHCP) server configuration, use the **show dhcp** command.

show dhcp {**leases** | **summary** | *scope*}

Syntax Description

leases	Displays allocated DHCP leases.
summary	Displays DHCP summary information.
scope	Name of a scope to display the DHCP information for that scope.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the allocated DHCP leases:

```
(Cisco Controller) >show dhcp leases
No leases allocated.
```

The following example shows how to display the DHCP summary information:

```
(Cisco Controller) >show dhcp summary
Scope Name           Enabled           Address Range
003                    No            0.0.0.0 -> 0.0.0.0
```

The following example shows how to display the DHCP information for the scope 003:

```
(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

To display the status of DHCP proxy handling, use the **show dhcp proxy** command.

show dhcp proxy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the status of DHCP proxy information:

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behavior: enabled
```

show dhcp timeout

To display the DHCP timeout value, use the **show dhcp timeout** command.

show dhcp timeout

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the DHCP timeout value:

```
(Cisco Controller) >show dhcp timeout

DHCP Timeout (seconds)..... 10
```

show dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show dtls connections** command.

show dtls connections

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show dtls connections** command.

```
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

To display a summary of all clients on the manual exclusion list from associating with the controller, use the **show exclusionlist** command.

show exclusionlist

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command displays all manually excluded MAC addresses.

The following example shows how to display the exclusion list:

```
(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
```

Related Commands

config exclusionlist

show fabric summary

To check the status of fabric, MAP server ip details, VNID mappings and timers, use the **show fabric summary** command.

show fabric summary

Syntax Description

This command has no keywords or arguments.

Command History

Release	Modification
8.5	This command was introduced.

Example

The following example shows how to view the fabric status, MAP server ip details, VNID mappings, and timers:

```
(Controller) >show fabric summary

Fabric Support................................. enabled

Enterprise Control Plane MS config
--------------------------------------

Primary Active MAP Server
IP Address..................................... 209.165.200.10
Preshared Key.................................. secret

Guest Control Plane MS config
-----------------------------
VNID Mappings configured: 6

Name                     L2-Vnid     L3-Vnid     IP Address/Subnet
---------------------  ----------  ----------  --------------------------
eid_9_6_51_0              10          100         9.6.51.0 / 255.255.255.0
eid_9_7_0_0               10          100         9.7.0.0 / 255.255.0.0
eid_9_6_53_0               1           0           0.0.0.0 / 0.0.0.0
eid_9_6_52_0             100           0           0.0.0.0 / 0.0.0.0
eid_9_6_54_0             100           25          1.2.3.4 / 255.255.255.0

anky                      23          0           0.0.0.0 / 0.0.0.0


Fabric Flex-Acl-tables           Status
-------------------------------- -------


Fabric Enabled Wlan summary
WLAN ID  WLAN Profile Name / SSID   Vnid    Encap    Tag      Peer ip
-------  ----------------------  --------- -----  -------  ---------------
6        testingA_6 / testingA_6     8        1      0        0.0.0.0
8        testingB_8 / testingB_8     80       1      0        0.0.0.0
17       TestA_17 / TestA_17         2        1      10       0.0.0.0
34       testingC_34 / testingC_34   2        1      0        0.0.0.0
```

```
35        testingD_35 / testingD_35   1         1       0         0.0.0.0
```

show flexconnect acl detailed

To display a detailed summary of FlexConnect access control lists, use the **show flexconnect acl detailed** command.

show flexconnect acl detailed *acl-name*

Syntax Description

acl-name	Name of the access control list.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the FlexConnect detailed ACLs:

```
(Cisco Controller) >show flexconnect acl detailed acl-2
```

show flexconnect acl summary

To display a summary of all access control lists on FlexConnect access points, use the **show flexconnect acl summary** command.

show flexconnect acl summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the FlexConnect ACL summary:

```
(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

To display details of a FlexConnect group, use the **show flexconnect group detail** command.

show flexconnect group detail {*group_name* | *default-flex-group*} | [**module-vlan** | **aps**]

Syntax Description

group_name	Name of the FlexConnect group.
module-vlan	Displays status of the FlexConnect local switching and VLAN ID in the group
aps	Displays list of APs that are part of the FlexConnect group
default-flex-group	Displays configuration of the default-flexgroup and the APs that are part of it.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.1	The **module-vlan** and **aps** parameters were added.
8.3	The *default-flex-group* option was added.

The following example shows how to display the detailed information for a specific FlexConnect group:

```
(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

To display the current list of FlexConnect groups, use the **show flexconnect group summary** command.

show flexconnect group summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the current list of FlexConnect groups:

```
(Cisco Controller) >show flexconnect group summary
flexconnect Group Summary:  Count 1
Group Name         # APs
Group 1       1
```

show flexconnect office-extend

To view information about OfficeExtend access points that in FlexConnect mode, use the **show flexconnect office-extend** command.

show flexconnect office-extend {**summary** | **latency**}

Syntax Description

summary	Displays a list of all OfficeExtend access points.
latency	Displays the link delay for OfficeExtend access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about the list of FlexConnect OfficeExtend access points:

```
(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
```

The following example shows how to display the FlexConnect OfficeExtend access point's link delay:

```
(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

To display the details or the statistics of the flow exporter, use the **show flow exporter** command.

show flow exporter {**summary** | **statistics**}

Syntax Description

summary	Displays a summary of the flow exporter.
statistics	Displays the statistics of flow exporters such as the number of records sent, or the time when the last record was sent.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show flow exporter summary** command:

```
(Cisco Controller) > show flow exporter summary
 Exporter-Name            Exporter-IP     Port
  =============            ===========     =====
  expo1                    9.9.120.115       800
```

show flow monitor summary

To display the details of the NetFlow monitor, use the **show flow monitor summary** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Netflow record monitoring and export are used for integration with an NMS or any Netflow analysis tool.

The following is a sample output of the **show flow monitor summary**:

```
(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

To display the configuration of a specific wired guest LAN, use the **show guest-lan** command.

show guest-lan *guest_lan_id*

Syntax Description

guest_lan_id	ID of the selected wired guest LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To display all wired guest LANs configured on the controller, use the **show guest-lan summary** command.

The following is a sample output of the **show guest-lan** *guest_lan_id* command:

```
(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

To display a summary of the icons present in the flash memory of the system, use the **show icons summary** command.

show icons summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
Release 8.2	This command was introduced.

The following is sample output from the **show icons summary** command::

```
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

To display active Internet Key Exchange (IKE) security associations (SAs), use the **show ike** command.

show ike {**brief** | **detailed**} *IP_or_MAC_address*

Syntax Description

brief	Displays a brief summary of all active IKE SAs.
detailed	Displays a detailed summary of all active IKE SAs.
IP_or_MAC_address	IP or MAC address of active IKE SA.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the active Internet Key Exchange security associations:

```
(Cisco Controller) > show ike brief 209.165.200.254
```

show interface summary

To display summary details of the system interfaces, use the **show interface summary** command.

show interface summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command was updated and displays IPv6 related details

The following example displays the summary of the local IPv4 interfaces:

```
(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
```

The following example displays the summary of the local IPv6 interfaces:

```
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

To display details of the system interfaces, use the **show interface** command.

show interfacedetailed {*interface_name* | **management** | **redundancy-management** | **redundancy-port** | **service-port** | **virtual**}

Syntax Description

detailed	Displays detailed interface information.
interface_name	Interface name for detailed display.
management	Displays detailed management interface information.
redundancy-management	Displays detailed redundancy management interface information.
redundancy-port	Displays detailed redundancy port information.
service-port	Displays detailed service port information.
virtual	Displays detailed virtual gateway interface information.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command was updated in Release 8.0 and displays IPv6 related details

The following example shows how to display the detailed interface information:

```
(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
```

Note Some WLAN controllers may have only one physical port listed because they have only one physical port.

The following example shows how to display the detailed redundancy management interface information:

```
(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
```

The following example shows how to display the detailed redundancy port information:

```
(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
```

The following example shows how to display the detailed service port information:

```
(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
```

The following example shows how to display the detailed virtual gateway interface information:

```
(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

To display details of system interface groups, use the **show interface group** command.

show interface group {**summary** | **detailed** *interface_group_name*}

Syntax Description

summary	Displays a summary of the local interface groups.
detailed	Displays detailed interface group information.
interface_group_name	Interface group name for a detailed display.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of local interface groups:

```
(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
```

The following example shows how to display the detailed interface group information:

```
(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

To see any ignored commands or invalid configuration values in an edited configuration file, use the **show invalid-config** command.

show invalid-config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You can enter this command only before the **clear config** or **save config** command.

The following is a sample output of the **show invalid-config** command:

```
(Cisco Controller) > show invalid-config
config wlan peer-blocking drop 3
config wlan dhcp_server 3 192.168.0.44 required
```

show inventory

To display a physical inventory of the Cisco wireless LAN controller, use the **show inventory** command.

show inventory

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Some wireless LAN controllers may have no crypto accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The following is a sample output of the **show inventory** command:

```
(Cisco Controller) > show inventory
Burned-in MAC Address.......................... 50:3D:E5:1A:31:A0
Power Supply 1................................. Present, OK
Power Supply 2................................. Absent
Maximum number of APs supported................ 500
NAME: "Chassis"    , DESCR: "Cisco 5500 Series Wireless LAN Controller"
PID: AIR-CT5508-K9,  VID: V01,  SN: XXXXXXXXXXX
```

show IPsec

To display active Internet Protocol Security (IPsec) security associations (SAs), use the **show IPsec** command.

show IPsec {**brief** | **detailed**} *IP_or_MAC_address*

Syntax Description

brief	Displays a brief summary of active IPsec SAs.
detailed	Displays a detailed summary of active IPsec SAs.
IP_or_MAC_address	IP address or MAC address of a device.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display brief information about the active Internet Protocol Security (IPsec) security associations (SAs):

```
(Cisco Controller) > show IPsec brief 209.165.200.254
```

Related Commands

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

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

show ipv6 acl detailed {*acl_name* | **summary**}

Syntax Description

acl_name	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
detailed	Displays detailed information about a specific ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed information of the access control lists:

```
(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

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

show ipv6 summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example displays the output of the **show ipv6 summary** command:

```
(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

To display the configuration of a specific wired guest LAN, use the **show guest-lan** command.

show guest-lan *guest_lan_id*

Syntax Description

guest_lan_id	ID of the selected wired guest LAN.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

To display all wired guest LANs configured on the controller, use the **show guest-lan summary** command.

The following is a sample output of the **show guest-lan** *guest_lan_id* command:

```
(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

To display icon parameters, use the **show icons file-info** command.

show icons file-info

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
Release 8.2	This command was introduced.

The following is sample output from the **show icons file-info** command:

```
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

To display the IPv6 access control lists (ACLs) that are configured on the controller, use the **show ipv6 acl** command.

show ipv6 acl detailed {*acl_name* | **summary**}

Syntax Description

acl_name	IPv6 ACL name. The name can be up to 32 alphanumeric characters.
detailed	Displays detailed information about a specific ACL.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed information of the access control lists:

```
(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

To display the IPv6 ACL CPU details, use the **show ipv6 acl cpu** command.

show ipv6 acl cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports IPv6 address format.

The following is a sample output of the **show ipv6 acl cpu** command:

```
(Cisco Controller) > show ipv6 acl cpu

CPU Acl Name.............................. NOT CONFIGURED
Wireless Traffic.......................... Disabled
Wired Traffic............................. Disabled
```

show ipv6 acl detailed

To display the IPv6 ACL details, use the **show ipv6 acl detailed** command.

show ipv6 acl detailed

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports IPv6 address format.

The following is a sample output of the **show ipv6 acl detailed TestACL** command:

```
(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

To display the IPv6 neighbor binding data that are configured on the controller, use the **show ipv6 neighbor-binding** command.

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**}

Syntax Description

capture-policy	Displays IPv6 next-hop message capture policies.
counters	Displays IPv6 next-hop counters (Bridging mode only).
detailed	Displays the IPv6 neighbor binding table.
mac	Displays the IPv6 binding table entries for a specific MAC address.
mac_address	Displays the IPv6 binding table entries for a specific MAC address.
port	Displays the IPv6 binding table entries for a specific port.
port_number	Port Number. You can enter ap for an access point or LAG for a LAG port.
vlan	Displays the IPv6 neighbor binding table entries for a specific VLAN.
vlan_id	VLAN identifier.
features	Displays IPv6 next-hop registered features.
policies	Displays IPv6 next-hop policies.
ra-throttle	Displays RA throttle information.
statistics	Displays RA throttle statistics.
routers	Displays RA throttle routers.
summary	Displays the IPv6 neighbor binding table.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

DHCPv6 counters are applicable only for IPv6 bridging mode.

The following is the output of the **show ipv6 neighbor-binding summary** command:

```
(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
```

The following is the output of the **show ipv6 neighbor-binding detailed** command:

```
(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
```

The following is the output of the **show ipv6 neighbor-binding counters** command:

```
(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

To display the RA guard statistics, use the **show ipv6 ra-guard** command.

show ipv6 ra-guard {**ap** | **wlc**} **summary**

Syntax Description

ap	Displays Cisco access point details.
wlc	Displays Cisco controller details.
summary	Displays RA guard statistics.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example show the output of the **show ipv6 ra-guard ap summary** command:

```
(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
```

The following example shows how to display the RA guard statistics for a controller:

```
(Cisco Controller) >show ipv6 ra-guard wlc summary
IPv6 RA Guard on WLC.................... Enabled
```

show ipv6 route summary

To display configuration information for IPv6 route, use the **show ipv6 route summary** command.

show ipv6 route summary

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced in a Release 8.0.

The following is a sample output of the **show ipv6 route summary** command:

```
(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

To display the IPv6 configuration settings, use the **show ipv6 summary** command.

show ipv6 summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example displays the output of the **show ipv6 summary** command:

```
(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

To display known Cisco lightweight access point information, use the **show known ap** command.

show known ap {**summary** | **detailed** *MAC*}

Syntax Description

summary	Displays a list of all known access points.
detailed	Provides detailed information for all known access points.
MAC	MAC address of the known AP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all known access points:

```
(Cisco Controller) >show known ap summary
MAC Address         State        # APs  # Clients   Last Heard
-----------         -----------  -----   --------   -----------------
```

Show Commands: j to q

- show l2tp, on page 1610
- show lag eth-port-hash, on page 1611
- show lag ip-port-hash, on page 1612
- show lag summary, on page 1613
- show ldap, on page 1614
- show ldap statistics, on page 1615
- show ldap summary, on page 1616
- show license all, on page 1617
- show license capacity, on page 1619
- show license detail, on page 1620
- show license expiring, on page 1621
- show license evaluation, on page 1622
- show license feature, on page 1623
- show license file, on page 1624
- show license handle, on page 1625
- show license image-level, on page 1626
- show license in-use, on page 1627
- show license permanent, on page 1628
- show license status, on page 1629
- show license statistics, on page 1630
- show license summary, on page 1631
- show license udi, on page 1632
- show license usage, on page 1633
- show load-balancing, on page 1634
- show local-auth config, on page 1635
- show local-auth statistics, on page 1637
- show local-auth certificates, on page 1639
- show logging, on page 1640
- show logging config-history, on page 1642
- show logging last-reset, on page 1643
- show logging flags, on page 1644
- show loginsession, on page 1645
- show macfilter, on page 1646

- show mdns ap summary, on page 1647
- show mdns domain-name-ip summary, on page 1648
- show mdns profile, on page 1650
- show mdns service , on page 1652
- show media-stream client, on page 1654
- show media-stream group detail, on page 1655
- show media-stream group summary, on page 1656
- show mesh ap, on page 1657
- show mesh astools stats, on page 1658
- show mesh backhaul, on page 1659
- show mesh bgscan, on page 1660
- show mesh cac, on page 1661
- show mesh client-access, on page 1663
- show mesh config, on page 1664
- show mesh env, on page 1665
- show mesh neigh, on page 1666
- show mesh path, on page 1669
- show mesh per-stats, on page 1670
- show mesh public-safety, on page 1671
- show mesh queue-stats, on page 1672
- show mesh security-stats, on page 1673
- show mesh stats, on page 1674
- show mgmtuser, on page 1675
- show mobility anchor, on page 1676
- show mobility ap-list, on page 1677
- show mobility foreign-map, on page 1678
- show mobility group member, on page 1679
- show mobility oracle, on page 1680
- show mobility statistics, on page 1682
- show mobility summary, on page 1683
- show msglog, on page 1685
- show nac statistics, on page 1686
- show nac summary, on page 1687
- show network, on page 1688
- show network summary, on page 1689
- show netuser, on page 1691
- show netuser guest-roles, on page 1692
- show network multicast mgid detail, on page 1693
- show network multicast mgid summary, on page 1694
- show network summary, on page 1695
- show nmsp notify-interval summary, on page 1697
- show nmsp status, on page 1698
- show nmsp statistics, on page 1699
- show nmsp subscription, on page 1701
- show nmsp subscription summary, on page 1702
- show ntp-keys, on page 1703

- show ntp-keys, on page 1704
- show opendns summary, on page 1705
- show pmk-cache, on page 1706
- show pmipv6 domain, on page 1707
- show pmipv6 mag bindings, on page 1708
- show pmipv6 mag globals, on page 1709
- show pmipv6 mag stats, on page 1710
- show pmipv6 profile summary, on page 1712
- show policy, on page 1713
- show port, on page 1715
- show profiling policy summary, on page 1717
- show qos, on page 1720
- show qos qosmap, on page 1721
- show queue-info, on page 1722

show l2tp

To display Layer 2 Tunneling Protocol (L2TP) sessions, use the **show l2tp** command.

show l2tp {**summary** | *ip_address*}

Syntax Description

summary	Displays all L2TP sessions.
ip_address	IP address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all L2TP sessions:

```
(Cisco Controller) > show l2tp summary
LAC_IPaddr LTid LSid RTid RSid ATid ASid State
---------- ---- ---- ---- ---- ---- ---- -----
```

show lag eth-port-hash

To display the physical port used for specific MAC addresses, use the **show lag eth-port-hash** command.

show lag eth-port-hash *dest_MAC* [*source_MAC*]

Syntax Description

dest_MAC	MAC address to determine output port for non-IP packets.
source_MAC	(Optional) MAC address to determine output port for non-IP packets.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the physical port used for a specific MAC address:

```
(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

To display the physical port used for specific IP addresses, use the **show lag ip-port-hash** command.

show lag ip-port-hash *dest_IP* [*source_IP*]

Syntax Description

dest_IP	IP address to determine the output port for IP packets.
source_IP	(Optional) IP address to determine the output port for IP packets.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both— IPv4 and IPv6 addresses.

Usage Guidelines

For CAPWAP packets, enter the IP address of the access points. For EOIP packets, enter the IP address of the controller. For WIRED_GUEST packets, enter its IP address. For non-tunneled IP packets from controller, enter the destination IP address. For other non-tunneled IP packets, enter both destination and source IP addresses.

This command is applicable for both IPv4 and IPv6 addresses.

The following example shows how to display the physical port used for a specific IP address:

```
(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

To display the current link aggregation (LAG) status, use the **show lag summary** command.

show lag summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the current status of the LAG configuration:

```
(Cisco Controller) > show lag summary
LAG Enabled
```

show ldap

To display the Lightweight Directory Access Protocol (LDAP) server information for a particular LDAP server, use the **show ldap** command.

show ldap *index*

Syntax Description

index	LDAP server index. Valid values are from 1 to 17.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the detailed LDAP server information:

```
(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
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap summary

show ldap statistics

To display all Lightweight Directory Access Protocol (LDAP) server information, use the **show ldap statistics** command.

show ldap statistics

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the LDAP server statistics:

```
(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
...
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap

show ldap summary

show ldap summary

To display the current Lightweight Directory Access Protocol (LDAP) server status, use the **show ldap summary** command.

show ldap summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of configured LDAP servers:

```
(Cisco Controller) > show ldap summary
Idx  Server Address   Port  Enabled
---  ---------------  ----  -------
1    2.3.1.4          389   Yes
2    10.10.20.22      389   Yes
```

Related Commands

config ldap

config ldap add

config ldap simple-bind

show ldap statistics

show ldap

show license all

To display information for all licenses on the controllers, use the **show license all** command.

show license all

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display all the licenses:

```
> 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
```

This example shows how to view all the licenses on the Smart License mechanism:

```
(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

To display the maximum number of access points allowed for this license on the Cisco 5500 Series Controller, the number of access points currently joined to the controller, and the number of access points that can still join the controller, use the **show license capacity** command.

show license capacity

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license capacity:

```
> show license capacity
Licensed Feature    Max Count         Current Count     Remaining Count
------------------------------------------------------------------------
AP Count            250               47                203
```

Related Commands

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

To display details of a specific license on the Cisco 5500 Series Controller, use the **show license detail** command.

show license detail *license-name*

Syntax Description

license-name	Name of a specific license.

Command Default

None.

This example shows how to display the license details:

```
> 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
```

Related Commands

license install

show license agent

show license all

show license feature

show license image-level

show license summary

license modify priority

show license expiring

To display details of expiring licenses on the Cisco 5500 Series Controller, use the **show license expiring** command.

show license expiring

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the details of the expiring licenses:

```
> 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
```

Related Commands

license install

show license all

show license detail

show license in-use

show license summary

license modify priority

show license evaluation

show license evaluation

To display details of evaluation licenses on the Cisco 5500 Series Controller, use the **show license evaluation** command.

show license evaluation

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the details of the evaluation licenses:

```
> 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
```

Related Commands

license install

show license all

show license detail

show license expiring

show license in-use

show license summary

license modify priority

show license feature

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license feature** command.

show license feature

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license-enabled features:

```
> 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
```

Related Commands

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

To display a summary of license-enabled features on the Cisco 5500 Series Controller, use the **show license file** command.

show license file

Syntax Description

This command has no arguments or keywords.

This example shows how to display the license files:

```
> 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=
. . .
```

Related Commands

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

To display the license handles on the Cisco 5500 Series Controller, use the **show license handle** command.

show license handle

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license handles:

```
> 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
```

Related Commands

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

To display the license image level that is in use on the Cisco 5500 Series Controller, use the **show license image-level** command.

show license image-level

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the image level license settings:

```
> 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.
```

Related Commands

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

To display the licenses that are in use on the Cisco 5500 Series Controller, use the **show license in-use** command.

show license in-use

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the licenses that are in use:

```
> 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
```

Related Commands

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

To display the permanent licenses on the Cisco 5500 Series Controller, use the **show license permanent** command.

show license permanent

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the permanent license's information:

```
> 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
```

Related Commands

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

To display the license status on the Cisco Wireless Controller, use the **show license status** command.

show license status

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to view the **license status** on the RTU license mechanism:

```
> 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
```

This example shows how to view the **license status** on the Smart License mechanism:

```
(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

To display license statistics on the Cisco 5500 Series Controller, use the **show license statistics** command.

show license statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the license statistics:

```
> 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
```

Related Commands

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

To see a brief summary of all licenses on the controllers, use the **show license summary** command.

show license summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a brief summary of all licenses:

```
> 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
```

This example shows how to view the **license summary** on the Smart License mechanism:

```
(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

To display unique device identifier (UDI) values for licenses on the controllers, use the **show license udi** command.

show license udi

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to view the UDI values for licenses on the RTU license mechanism:

```
(Cisco Controller) > show license udi
Device# PID                   SN                    UDI
------------------------------------------------------------------------------
*0      AIR-CT5508-K9         RFD000P2D27           AIR-CT5508-K9:RFD000P2D27
```

This example shows how to view the UDI values for licenses on the Smart License mechanism:

```
(Cisco Controller) > show license udi

UDI: PID:AIR-CTVM-K9,SN:91U8NQ5XDBE
```

show license usage

To display the entitlement details and usage per handle and its entitlement tag, use the **show license usage** command.

show license usage

Command History

Release	Modification
8.2	This command was introduced in a 8.2 release.

This example shows how to display the entitlement details:

```
(Cisco Controller) >show license usage
```

show load-balancing

To display the status of the load-balancing feature, use the **show load-balancing** command.

show load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the load-balancing status:

```
> 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
```

Related Commands

config load-balancing

show local-auth config

To display local authentication configuration information, use the **show local-auth config** command.

show local-auth config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the local authentication configuration information:

```
(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
```

Related Commands

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

To display local Extensible Authentication Protocol (EAP) authentication statistics, use the **show local-auth statistics** command:

show local-auth statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the local authentication certificate statistics:

```
(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
```

Related Commands

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

To display local authentication certificate information, use the **show local-auth certificates** command:

show local-auth certificates

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the authentication certificate information stored locally:

```
(Cisco Controller) > show local-auth certificates
```

Related Commands

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

To display the syslog facility logging parameters and buffer contents, use the **show logging** command.

show logging

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the current settings and buffer content details:

```
(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

To view all the **config** commands executed from the time of reboot, use the **show logging config-history** command. This command is useful to understand the timestamp of execution of these commands, order of occurrence, source of command execution, and executed command history, which are lost after controller reboot or after you clear all the configuration.

show logging config-history

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
8.8	This command was introduced.

show logging last-reset

To display the logging buffer saved on last reset or power cycle of the controller, use the **show logging last-reset** command.

show logging last-reset

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced in 8.0.140.0.

show logging flags

To display the existing flags, use the **show logging flags** command.

show logging flags *AP* | *Cilent*

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current flags details:

```
> show logging flags
ID    username      Connection From   Idle Time    Login Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

Related Commands

config logging flags close

show loginsession

To display the existing sessions, use the **show loginsession** command.

show loginsession

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current session details:

```
> show loginsession
ID    username     Connection From   Idle Time    Session Time
-- ---------------  ---------------  ------------  ------------
00 admin            EIA-232          00:00:00      00:19:04
```

Related Commands

config loginsession close

show macfilter

To display the MAC filter parameters, use the **show macfilter** command.

show macfilter {**summary** | **detail***MAC* | **mesh** | {**wlan** *wlan-id*}}

Syntax Description

summary	Displays a summary of all MAC filter entries.
detail *MAC*	Displays details of a MAC filter entry.
mesh	Display a summary of all MESH AP MAC filter entries.
wlan *wlan-id*	Display a summary of all MAC filter entries on given wlan.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.4	**wlan** *wlan-id* was added.

Usage Guidelines

The MAC delimiter (none, colon, or hyphen) for MAC addresses sent to RADIUS servers is displayed. The MAC filter table lists the clients that are always allowed to associate with a wireless LAN.

The following example shows how to display the detailed display of a MAC filter entry:

```
(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
```

The following example shows how to display a summary of the MAC filter parameters:

```
(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

To display all the access points for which multicast Domain Name System (mDNS) forwarding is enabled, use the **show mnds ap summary** command.

show mdns ap summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show mnds ap summary** command:

```
(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
```

The following table describes the significant fields shown in the display.

Table 13: show mdns ap summary Field Descriptions

Field	Description
AP Name	Name of the mDNS access point (access point for which mDNS forwarding is enabled).
Ethernet MAC	MAC address of the mDNS access point.
Number of VLANs	Number of VLANs from which the access point snoops the mDNS advertisements from the wired side. An access point can snoop on a maximum of 10 VLANs.
VLAN Identifiers	Identifiers of the VLANs the access point snoops on.

show mdns domain-name-ip summary

To display the summary of the multicast Domain Name System (mDNS) domain names, use the **show mdns domain-name-ip summary** command.

show mdns domain-name-ip summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

Usage Guidelines

Each service advertisement contains a record that maps the domain name of the service provider to the IP address. The mapping also contains details such as the client MAC address, VLAN ID, Time to Live (TTL), and IPv4 address.

The following is a sample output of the **show mdns domain-name-ip summary** command:

```
(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
```

The following table describes the significant fields shown in the display.

Table 14: show mdns domain-name-ip summary Field Descriptions

Field	Description
Domain Name	Domain name of the service provider.
MAC Address	MAC address of the service provider.
IP Address	IP address of the service provider.
VLAN ID	VLAN ID of the service provider.

Field	Description
Type	Origin of service that can be one of the following: • Wired • Wireless • Wired guest • mDNS AP
TTL	TTL value, in seconds, that determines the validity of the service offered by the service provider. The service provider is removed from the controller when the TTL expires.
Time Left	Time remaining, in seconds, before the service provider is removed from the controller.

show mdns profile

To display mDNS profile information, use the **show mdns profile** command.

show mdns profile {**summary** | **detailed** *profile-name*}

Syntax Description

summary	Displays the summary of the mDNS profiles.
detailed	Displays details of an mDNS profile.
profile-name	Name of the mDNS profile.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.

This example shows how to display a summary of all the mDNS profiles:

```
> show mdns profile summary
Number of Profiles.............................. 2

ProfileName                       No. Of Services
--------------------------------  ---------------
default-mdns-profile                   5
profile1                               2
```

This example shows how to display the detailed information of an mDNS profile:

```
> 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
```

Related Commands

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

To display multicast Domain Name System (mDNS) service information, use the **show mnds service** command.

show mdns service {**summary** | **detailed** *service-name* | **not-learnt**}

Syntax Description

summary	Displays the summary of all mDNS services.
detailed	Displays the details of an mDNS service.
service-name	Name of the mDNS service.
not-learnt	Displays the summary of all the service advertisements that were received by the controller but were not discovered because the service query status was disabled. Service advertisements for all VLANs and origin types that are not learned are displayed in the output. The top 500 services appear in the summary list.

Command Default

None

Command History

Release	Modification
7.4	This command was introduced.
7.5	The **not-learnt** keyword was added.

The following is a sample output of the **show mnds summary** command:

```
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.
```

The following is a sample output of the **show mnds service detailed** command:

```
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
```

The following is a sample output of the **show mnds service not-learnt**command:

```
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

To display the details for a specific media-stream client or a set of clients, use the **show media-stream client** command.

show media-stream client {*media-stream_name* | **summary**}

Syntax Description

media-stream_name	Name of the media-stream client of which the details is to be displayed.
summary	Displays the details for a set of media-stream clients.

Command Default

None.

This example shows how to display a summary media-stream clients:

```
> 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
```

Related Commands

show media-stream group summary

show media-stream group detail

To display the details for a specific media-stream group, use the **show media-stream group detail** command.

show media-stream group detail *media-stream_name*

Syntax Description

media-stream_name	Name of the media-stream group.

Command Default

None.

This example shows how to display media-stream group configuration details:

```
> 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
```

Related Commands

show media-stream group summary

show media-stream group summary

To display the summary of the media stream and client information, use the **show media-stream group summary** command.

show media-stream group summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display a summary of the media-stream group:

```
(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
```

Related Commands

show 802.11 media-stream client

show media-stream client

show media-stream group detail

show mesh ap

To display settings for mesh access points, use the **show mesh ap** command.

show mesh ap {**summary** | **tree**}

Syntax Description

summary	Displays a summary of mesh access point information including the name, model, bridge virtual interface (BVI) MAC address, United States Computer Emergency Response Team (US-CERT) MAC address, hop, and bridge group name.
tree	Displays a summary of mesh access point information in a tree configuration, including the name, hop counter, link signal-to-noise ratio (SNR), and bridge group name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary format:

```
(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
```

The following example shows how to display settings in a hierarchical (tree) format:

```
(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

To display antistranding statistics for outdoor mesh access points, use the **show mesh astools stats** command.

show mesh astools stats [*cisco_ap*]

Syntax Description

cisco_ap	(Optional) Antistranding feature statistics for a designated mesh access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display anti-stranding statistics on all outdoor mesh access points:

```
(Cisco Controller) >show mesh astools stats
Total No of Aps stranded : 0
```

The following example shows how to display anti-stranding statistics for access point *sb_map1*:

```
(Cisco Controller) >show mesh astools stats sb_map1
Total No of Aps stranded : 0
```

show mesh backhaul

To check the current backhaul information, use the **show mesh backhaul** command.

show mesh backhaul *cisco_ap*

Syntax Description

cisco_ap	Name of the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the current backhaul:

```
(Cisco Controller) >show mesh backhaul
```

If the current backhaul is 5 GHz, the output is as follows:

```
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 bgscan

To see the details of mesh background scan, use the **show mesh bgscan** command.

show mesh bgscan

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.3	This command was introduced.

Example

```
Cisco Controller# show mesh bgscan

Background Scanning: enabled

Off Channel Neighbors
---------------------
Channel:165
Mac:5835.d9aa.9acf MissCnt:0 NDRespCnt:1078 HopCnt:1 AdjustedEase:4096
Flags: NEIGH BEACON
Mac:5017.ffdc.2eaf MissCnt:0 NDRespCnt:38 HopCnt:1 AdjustedEase:18648576 StickyEase:23448576

Flags: NEIGH PARENT BEACON

Channel:157
Mac:ece1.a930.bc8f MissCnt:0 NDRespCnt:5 HopCnt:1 AdjustedEase:3048576
Flags: NEIGH BEACON

Channel:161
Mac:f8c2.8883.fadf MissCnt:0 NDRespCnt:20 HopCnt:1 AdjustedEase:262144
Flags: NEIGH

Aligned Offchannel neighbors
----------------------------

Channel:165 (ON-CHANNEL)
Mac:5017.ffdc.2eaf Ease:18648576
Mac:5835.d9aa.9acf Ease:4096
Channel:157 (POTENTIAL OFFCHAN
NEL)
Mac:ece1.a930.bc8f Ease:3048576
Mac:0021.d8d6.a6cf Ease:0

Channel:161
Mac:f8c2.8883.fadf Ease:262144
```

show mesh cac

To display call admission control (CAC) topology and the bandwidth used or available in a mesh network, use the **show mesh cac** command.

show mesh cac {**summary** | {**bwused** {**voice** | **video**} | **access** | **callpath** | **rejected**} *cisco_ap*}

Syntax Description

summary	Displays the total number of voice calls and voice bandwidth used for each mesh access point.
bwused	Displays the bandwidth for a selected access point in a tree topology.
voice	Displays the mesh topology and the voice bandwidth used or available.
video	Displays the mesh topology and the video bandwidth used or available.
access	Displays access voice calls in progress in a tree topology.
callpath	Displays the call bandwidth distributed across the mesh tree.
rejected	Displays voice calls rejected for insufficient bandwidth in a tree topology.
cisco_ap	Mesh access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the call admission control settings:

```
(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
```

The following example shows how to display the mesh topology and the voice bandwidth used or available:

```
(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
```

The following example shows how to display the access voice calls in progress in a tree topology:

```
(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

To display the backhaul client access configuration setting, use the **show mesh client-access** command.

show mesh client-access

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display backhaul client access configuration settings for a mesh access point:

```
(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

To display mesh configuration settings, use the **show mesh config** command.

show mesh config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display global mesh configuration settings:

```
(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
```

show mesh env

To display global or specific environment summary information for mesh networks, use the **show mesh env** command.

show mesh env {**summary** | *cisco_ap*}

Syntax Description

summary	Displays global environment summary information.
cisco_ap	Name of access point for which environment summary information is requested.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display global environment summary information:

```
(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
```

The following example shows how to display an environment summary for an access point:

```
(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

To display summary or detailed information about the mesh neighbors of a mesh access point, use the **show mesh neigh** command.

show mesh neigh {**detail** | **summary**} {*cisco_ap* | **all**}

Syntax Description

detail	Displays the channel and signal-to-noise ratio (SNR) details between the designated mesh access point and its neighbor.
summary	Displays the mesh neighbors for a designated mesh access point.
cisco_ap	Cisco lightweight access point name.
all	Displays all access points.

Note If an AP itself is configured with the **all**keyword, the **all**keyword access points take precedence over the AP that is named **all**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a neighbor summary of an access point:

```
(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
```

The following example shows how to display the detailed neighbor statistics of an access point:

```
(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
```

The following table lists the output flags displayed for the **show mesh neigh detail** command.

Table 15: Output Flags for the show mesh neigh detail command

Output Flag	Description
AP MAC	MAC address of a mesh neighbor for a designated mesh access point.
AP Name	Name of the mesh access point.
FLAGS	Describes adjacency. The possible values are as follows: • UPDATED—Recently updated neighbor. • NEIGH—One of the top neighbors. • EXCLUDED—Neighbor is currently excluded. • WASEXCLUDED—Neighbor was recently removed from the exclusion list. • PERMSNR—Permanent SNR neighbor. • CHILD—A child neighbor. • PARENT—A parent neighbor. • NEEDUPDATE—Not a current neighbor and needs an update. • BEACON—Heard a beacon from this neighbor. • ETHER—Ethernet neighbor.
worstDv	Worst distance vector through the neighbor.
Ant	Antenna on which the route was received.
channel	Channel of the neighbor.
biters	Number of black list timeouts left.
ppiters	Number of potential parent timeouts left.
Numroutes	Number of distance routes.
snr	Signal to Noise Ratio.
snrUp	SNR of the link to the AP.
snrDown	SNR of the link from the AP.
linkSnr	Calculated SNR of the link.
adjustedEase	Ease to the root AP through this AP. It is based on the current SNR and threshold SNR values.
unadjustedEase	Ease to the root AP through this AP after applying correct for number of hops.
txParent	Packets sent to this node while it was a parent.
rxparent	Packets received from this node while it was a parent.

Output Flag	Description
poorSnr	Packets with poor SNR received from a node.
lastUpdate	Timestamp of the last received message for this neighbor
parentChange	When this node last became parent.
per antenna smoother SNR values	SNR value is populated only for antenna 0.

show mesh path

To display the channel and signal-to-noise ratio (SNR) details for a link between a mesh access point and its neighbor, use the **show mesh path** command.

show mesh path *cisco_ap*

Syntax Description

cisco_ap	Mesh access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display channel and SNR details for a designated link path:

```
(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

To display the percentage of packet errors for packets transmitted by the neighbors of a specified mesh access point, use the **show mesh per-stats** command.

show mesh per-stats summary {*cisco_ap* | **all**}

Syntax Description

summary	Displays the packet error rate stats summary.
cisco_ap	Name of mesh access point.
all	Displays all mesh access points.

Note If an AP itself is configured with the **all**keyword, the **all**keyword access points take precedence over the AP that is named **all**.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The packet error rate percentage equals 1, which is the number of successfully transmitted packets divided by the number of total packets transmitted.

The following example shows how to display the percentage of packet errors for packets transmitted by the neighbors to a mesh access point:

```
(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

To display 4.8-GHz public safety settings, use the **show mesh public-safety** command.

show mesh public-safety

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to view 4.8-GHz public safety settings:

```
(Cisco Controller) >(Cisco Controller) >show mesh public-safety
Global Public Safety status: disabled
```

show mesh queue-stats

To display the number of packets in a client access queue by type for a mesh access point, use the **show mesh queue-stats** command.

show mesh queue-stats {*cisco_ap* | **all**}

Note If an AP itself is configured with the **all**keyword, the **all**keyword access points take precedence over the AP that is named **all**.

Syntax Description

cisco_ap	Name of access point for which you want packet queue statistics.
all	Displays all access points.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display packet queue statistics for access point ap417:

```
(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

To display packet error statistics for a specific access point, use the **show mesh security-stats** command.

show mesh security-stats {*cisco_ap* | **all**}

Syntax Description

cisco_ap	Name of access point for which you want packet error statistics.
all	Displays all access points.

Note If an AP itself is configured with the **all** keyword, the **all** keyword access points take precedence over the AP that is named **all**.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command shows packet error statistics and a count of failures, timeouts, and successes with respect to associations and authentications as well as reassociations and reauthentications for the specified access point and its child.

The following example shows how to view packet error statistics for access point ap417:

```
(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

To display the mesh statistics for an access point, use the **show mesh stats** command.

show mesh stats *cisco_ap*

Syntax Description

cisco_ap	Access point name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display statistics of an access point:

```
(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

To display the local management user accounts on the Cisco wireless LAN controller, use the **show mgmtuser** command.

show mgmtuser

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a list of management users:

```
> show mgmtuser
User Name                 Permissions    Description            Password Strength
-----------------------   ------------   --------------         ------------------
admin                     read-write                                    Weak
```

Related Commands

config mgmtuser add

config mgmtuser delete

config mgmtuser description

config mgmtuser password

show mobility anchor

To display the wireless LAN anchor export list for the Cisco wireless LAN controller mobility groups or to display a list and status of controllers configured as mobility anchors for a specific WLAN or wired guest LAN, use the **show mobility anchor** command.

show mobility anchor [**wlan** *wlan_id* | **guest-lan** *guest_lan_id*]

Syntax Description

wlan	(Optional) Displays wireless LAN mobility group settings.
wlan_id	Wireless LAN identifier from 1 to 512 (inclusive).
guest-lan	(Optional) Displays guest LAN mobility group settings.
guest_lan_id	Guest LAN identifier from 1 to 5 (inclusive).

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The status field display (see example) shows one of the following values:

- UP—The controller is reachable and able to pass data.
- CNTRL_PATH_DOWN—The mpings failed. The controller cannot be reached through the control path and is considered failed.
- DATA_PATH_DOWN—The epings failed. The controller cannot be reached and is considered failed.
- CNTRL_DATA_PATH_DOWN—Both the mpings and epings failed. The controller cannot be reached and is considered failed.

The following example shows how to display a mobility wireless LAN anchor list:

```
(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

To display the mobility AP list, use the **show mobility ap-list** command.

show mobility ap-list

Syntax Description This command has no arguments or keywords.

Command Default None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the mobility AP list:

Note The AP name is displayed only with New Mobility. With Old Mobility, the AP name is displayed as `Unknown`.

```
(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

To display a mobility wireless LAN foreign map list, use the **show mobility foreign-map** command.

show mobility foreign-map wlan *wlan_id*

Syntax Description

wlan	Displays the mobility WLAN foreign-map list.
wlan_id	Wireless LAN identifier between 1 and 512.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to get a mobility wireless LAN foreign map list:

```
(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

To display the details of the mobility group members in the same domain, use the **show mobility group member** command.

show mobility group member hash

Syntax Description

hash	Displays the hash keys of the mobility group members in the same domain.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the hash keys of the mobility group members:

```
(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

To display the status of the mobility controllers known to the Mobility Oracle (MO) or display the details of the MO client database, use the **show mobility oracle** command.

show mobility oracle {**client** {**detail** | **summary**} | **summary**}

Syntax Description

client	Displays the MO client database.
detail	Displays details pertaining to a client in MO client database.
summary	Displays the summary of the MO database.

Command Default

None

Command History

Release	Modification
7.3.112.0	This command was introduced.

The following is a sample output of the **show mobility oracle summary** command:

```
(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
```

The following is a sample output of the **show mobility oracle client summary** command:

```
(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
```

The following is a sample output of the **show mobility oracle client detail** command:

```
(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

To display the statistics information for the Cisco wireless LAN controller mobility groups, use the **show mobility statistics** command.

show mobility statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display statistics of the mobility manager:

```
(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

To display the summary information for the controller mobility groups, use the **show mobility summary** command.

show mobility summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Some WLAN controllers may list no mobility security mode.

The following is a sample output of the **show mobility summary** command.

```
(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
```

The following is a sample output of the **show mobility summary** command with new mobility architecture.

```
(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

To display the message logs written to the controller database, use the **show msglog** command.

show msglog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

If there are more that 15 entries, you are prompted to display the messages shown in the example.

The following example shows how to display message logs:

```
 (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

To display detailed Network Access Control (NAC) information about a Cisco wireless LAN controller, use the **show nac statistics** command.

show nac statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed statistics of network access control settings:

```
(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
```

Related Commands

show nac summary

config guest-lan nac

config wlan nac

debug nac

show nac summary

To display NAC summary information for a Cisco wireless LAN controller, use the **show nac summary** command.

show nac summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary information of network access control settings:

```
(Cisco Controller) > show nac summary
NAC ACL Name ..............................................
Index  Server Address                            Port     State
-----  ---------------------------------------   ----     -----
1      xxx.xxx.xxx.xxx                           13336    Enabled
```

Related Commands

show nac statistics

config guest-lan nac

config wlan nac

debug nac

show network

To display the current status of 802.3 bridging for all WLANs, use the **show network** command.

show network

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the network details:

```
(Cisco Controller) > show network
```

Related Commands

config network

show network summary

show network multicast mgid detail

show network multicast mgid summary

show network summary

To display the network configuration of the Cisco wireless LAN controller, use the **show network summary** command.

show network summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary configuration:

```
(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............................. Default
CAPWAP Prefer Mode.......................... IPv4
```

show netuser

To display the configuration of a particular user in the local user database, use the **show netuser** command.

show netuser {**detail** *user_name* | **guest-roles** | **summary**}

Syntax Description

detail	Displays detailed information about the specified network user.
user_name	Network user.
guest_roles	Displays configured roles for guest users.
summary	Displays a summary of all users in the local user database.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show netuser summary** command:

```
(Cisco Controller) > show netuser summary
Maximum logins allowed for a given username ........Unlimited
```

The following is a sample output of the **show netuser detail** command:

```
(Cisco Controller) > show netuser detail john10
username..................................... abc
WLAN Id...................................... Any
Lifetime..................................... Permanent
Description.................................. test user
```

Related Commands

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

To display a list of the current quality of service (QoS) roles and their bandwidth parameters, use the **show netuser guest-roles** command.

show netuser guest-roles

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display a QoS role for the guest network user:

```
(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
```

Related Commands

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

To display all the clients joined to the multicast group in a specific multicast group identification (MGID), use the **show network multicast mgid detail** command.

show network multicast mgid detail *mgid_value*

Syntax Description

mgid_value	Number between 550 and 4095.

Command Default

None.

This example shows how to display details of the multicast database:

```
> 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
```

Related Commands

show network summary

show network multicast mgid detail

show network

show network multicast mgid summary

To display all the multicast groups and their corresponding multicast group identifications (MGIDs), use the **show network multicast mgid summary** command.

show network multicast mgid summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary of multicast groups and their MGIDs:

```
> 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
```

Related Commands

show network summary

show network multicast mgid detail

show network

show network summary

To display the network configuration settings, use the **show network summary** command.

show network summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command updated to display the IPv6 multicast details in the network summary.

The following example displays the output of the **show ipv6 summary** command:

```
(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

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp notify-interval summary** command.

show nmsp notify-interval summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display NMSP configuration settings:

```
> 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
```

Related Commands

clear locp statistics

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp statistics

show nmsp status

show nmsp status

To view the active NMSP connections status, use the **show nmsp status**command.

show nmsp status

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows the active nmsp connections status:

```
(Cisco Controller) >show nmsp status
```

show nmsp statistics

To display Network Mobility Services Protocol (NMSP) counters, use the **show nmsp statistics** command.

show nmsp statistics {**summary** | **connection all**}

Syntax Description

summary	Displays common NMSP counters.
connection all	Displays all connection-specific counters.

Command Default

None.

This example shows how to display a summary of common NMSP counters:

```
> 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
```

This example shows how to display all the connection-specific NMSP counters:

```
> 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
```

Related Commands

show nmsp notify-interval summary

clear nmsp statistics

config nmsp notify-interval measurement

show nmsp status

show nmsp subscription

To display the Network Mobility Services Protocol (NMSP) services that are active on the controller, use the **show nmsp subscription** command.

show nmsp subscription {**summary** | **detail** *ip-addr*}

Syntax Description

summary	Displays all of the NMSP services to which the controller is subscribed.
detail	Displays details for all of the NMSP services to which the controller is subscribed.
ip-addr	Details only for the NMSP services subscribed to by a specific IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

This example shows how to display a summary of all the NMSP services to which the controller is subscribed:

```
> show nmsp subscription summary
Mobility Services Subscribed:
Server IP          Services
---------          --------
10.10.10.31        RSSI, Info, Statistics
```

This example shows how to display details of all the NMSP services:

```
> 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

To view the mobility services subscribed on controller by Mobility Services Engine, use the **show nmsp subscription summary** command.

show nmsp subscription summary

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.3	This command was introduced.

This example shows the subscribed mobility services on controller:

```
(Cisco Controller) >show nmsp subscription summary
```

show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

show ntp-keys

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display NTP authentication key details:

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

Related Commands

config time ntp

show ntp-keys

To display network time protocol authentication key details, use the **show ntp-keys** command.

show ntp-keys

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display NTP authentication key details:

```
(Cisco Controller) > show ntp-keys
Ntp Authentication Key Details...................
      Key Index
     -----------
         1
         3
```

Related Commands

config time ntp

show opendns summary

To display OpenDNS configuration details, use the **show opendns summary** command.

show opendns summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
8.4	This command was introduced.

Example

The following example shows how to view an OpenDNS configuration:

```
(Cisco Controller) > show opendns summary

OpenDnsGlobalStatus.............................. Enabled
OpenDns-ApiToken................................. 12

  Profile-Name                    Device ID                State
  ============                    ==============           =============
  guest1                           010a8501693bf162        Profile Registered


Profiles Mapped to WLANIDs
==========================

Profile Name                     WLAN IDs (Mapped)
-----------------                -----------------
guest1                  7

Profiles Mapped to APGroup WLAN-IDs
===============================

Profile Name                    Site Name / WLAN IDs (Mapped)
-----------------                -----------------
guest1                  NONE

Profiles Mapped to Local Policies

--More-- or (q)uit
==========================

Profile Name                     Local Policies (Mapped)
-----------------                -----------------
guest1                  NONE
```

show pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show pmk-cache** command.

show pmk-cache {**all** | *MAC*}

Syntax Description

all	Displays information about all entries in the PMK cache.
MAC	Information about a single entry in the PMK cache.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about a single entry in the PMK cache:

```
(Cisco Controller) >show pmk-cache xx:xx:xx:xx:xx:xx
```

The following example shows how to display information about all entries in the PMK cache:

```
(Cisco Controller) >show pmk-cache all
PMK Cache
                    Entry
Station             Lifetime   VLAN Override          IP Override
-----------------   --------   --------------------   ---------------
```

show pmipv6 domain

To display the summary information of a PMIPv6 domain, use the **show pmipv6 domain** command.

show pmipv6 domain *domain_name* **profile** *profile_name*

Syntax Description

domain_name	Name of the PMIPv6 domain. The domain name can be up to 127 case-sensitive alphanumeric characters.
profile	Specifies the PMIPv6 profile.
profile_name	Name of the profile associated with the PMIPv6 domain. The profile name can be up to 127 case-sensitive alphanumeric characters.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the summary information of a PMIPv6 domain:

```
(Cisco Controller) >show pmipv6 domain floor1 profile profile1
NAI: @example.com
APN: Example
LMA: Examplelma

NAI: *
APN: ciscoapn
LMA: ciscolma
```

show pmipv6 mag bindings

To display the binding information of a Mobile Access Gateway (MAG), use the **show pmipv6 mag binding** command.

show pmipv6 mag bindings [**lma** *lma_name* | **nai** *nai_string*]

Syntax Description

lma	(Optional) Displays the binding details of the MAG to an Local Mobility Anchor (LMA).
lma_name	Name of the LMA. The LMA name is case-sensitive and can be up to 127 alphanumeric characters.
nai	(Optional) Displays the binding details of the MAG to a client.
nai_string	Network Access Identifier (NAI) of the client. The NAI is case-sensitive and can be up to 127 alphanumeric characters. You can use all special characters except a colon.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the MAG bindings:

```
(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

To display the global PMIPv6 parameters of the Mobile Access Gateway (MAG), use the **show pmipv6 mag globals** command.

show pmipv6 mag globals

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the global PMIPv6 parameters of a MAG:

```
(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

To display the statistics of the Mobile Access Gateway (MAG), use the **show pmipv6 mag stats** command.

show pmipv6 mag stats [**domain** *domain_name* **peer** *lma_name*]

Syntax Description

domain	(Optional) Displays the MAG statistics for a Local Mobility Anchor (LMA) in the domain.
domain_name	Name of the PMIPv6 domain. The domain name is case-sensitive and can be up to 127 alphanumeric characters.
peer	(Optional) Displays the MAG statistics for an LMA.
lma_name	Name of the LMA. The LMA name is case sensitive and can be up to 127 alphanumeric characters.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This table lists the descriptions of the LMA statistics.

Table 16: Descriptions of the LMA Statistics:

LMA Statistics	Description
PBU Sent	Total number of Proxy Binding Updates (PBUs) sent to the LMA by the MAG. PBU is a request message sent by the MAG to a mobile node's LMA for establishing a binding between the mobile node's interface and its current care-of address (Proxy-CoA).
PBA Received	Total number of Proxy Binding Acknowledgements (PBAs) received by the MAG from the LMA. PBA is a reply message sent by an LMA in response to a PBU message that it receives from a MAG.
PBRI Sent	Total number of Proxy Binding Revocation Indications (PBRIs) sent by the MAG to the LMA.
PBRI Received	Total number of PBRIs received from the LMA by the MAG.
PBRA Sent	Total number of Proxy Binding Revocation Acknowledgements (PBRAs) sent by the MAG to the LMA.
PBRA Received	Total number of PBRAs that the MAG receives from the LMA.
Number of Handoff	Number of handoffs between the MAG and the LMA.

The following example shows how to display the LMA statistics:

```
(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

To display the summary of the PMIPv6 profiles, use the **show pmipv6 profile summary** command.

show pmipv6 profile summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the summary of the PMIPv6 profiles:

```
(Cisco Controller) >show pmipv6 profile summary
 Profile Name    WLAN IDS (Mapped)
 ------------    -----------------
  Group1            6
```

show policy

To display the summary of the configured policies, and the details and statistics of a policy, use the **show policy** command.

show policy {**summary** | *policy-name* [**statistics**]}

Syntax Description

summary	Displays the summary of configured policies.
policy-name	Name of the policy.
statistics	(Optional) Displays the statistics of a policy.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show policy summary** command:

```
(Cisco Controller) > show policy summary

Number of Policies..... 2

Policy Index Policy Name
------------ ----------------
1            student-FullAccess
2            teacher-FullAccess
```

The following example shows how to display the details of a policy:

```
(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
```

The following example shows how to display the statistics of a policy:

```
(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

To see the controller port settings on an individual or global basis, use the **show port** command.

show port { *port-number* | **summary** | **detailed-info** | **vlan** }

Syntax Description

port-number	Port number of the physical interface.
summary	Displays a summary of all ports.
detailed-info	Displays detailed port information.
vlan	Displays VLAN port table summary.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about an individual controller port:

```
(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
```

Note Some controllers may not have multicast or Power over Ethernet (PoE) listed because they do not support those features.

The following example shows how to display a summary of all ports:

```
(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
```

Note Some controllers may have only one port listed because they have only one physical port.

show profiling policy summary

To display local device classification of the controller, use the **show profiling policy summary** command.

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show profiling policy summary** command:

```
(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

To display quality of service (QoS) information, use the **show qos** command.

show qos {**bronze** | **gold** | **platinum** | **silver**}

Syntax Description

bronze	Displays QoS information for the bronze profile of the WLAN.
gold	Displays QoS information for the gold profile of the WLAN.
platinum	Displays QoS information for the platinum profile of the WLAN.
silver	Displays QoS information for the silver profile of the WLAN.

Command Default

None.

This example shows how to display QoS information for the gold profile:

```
> 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
```

Related Commands

config qos protocol-type

show qos qosmap

To see the current QoS map configuration, use the **show qos** command.

show qos qosmap

Syntax Description

qosmap	Displays the current QoS map

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows the current QoS map configuration:

```
show qos qosmap
```

show queue-info

To display all the message queue information pertaining to the system, use the **show queue-info** command.

show queue-info

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced.

The following is a sample output of the **show queue-info** command.

```
(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
```

The following table describes the significant fields shown in the display.

Table 17: show queue-info Field Descriptions

Field	Description
Queue Name	Name of the task message queue.
Allocated	Memory size, in bytes, of the message queue.
InUse	Queue that is currently used. A value of 0 indicates that there are no messages that have to be processed by the task.

Field	Description
MaxUsed	Maximum number of messages processed by the task after the controller is up.

Show Commands: r to z

- show radius acct detailed, on page 1728
- show radius acct statistics, on page 1729
- show radius auth detailed, on page 1730
- show radius auth statistics, on page 1731
- show radius avp-list, on page 1732
- show radius summary, on page 1733
- show redundancy interfaces, on page 1734
- show redundancy latency, on page 1735
- show redundancy mobilitymac, on page 1736
- show redundancy peer-route summary, on page 1737
- show redundancy peer-system statistics, on page 1738
- show redundancy statistics, on page 1739
- show redundancy summary, on page 1740
- show redundancy timers, on page 1741
- show remote-lan, on page 1742
- show reset, on page 1744
- show rfid client, on page 1745
- show rfid config, on page 1746
- show rfid detail, on page 1747
- show rfid summary, on page 1748
- show rf-profile summary, on page 1749
- show rf-profile details, on page 1750
- show rogue adhoc custom summary, on page 1753
- show rogue adhoc detailed, on page 1754
- show rogue adhoc friendly summary , on page 1755
- show rogue adhoc malicious summary, on page 1756
- show rogue adhoc unclassified summary , on page 1757
- show rogue adhoc summary, on page 1758
- show rogue ap clients, on page 1759
- show rogue ap custom summary , on page 1761
- show rogue ap detailed, on page 1763
- show rogue ap friendly summary, on page 1766
- show rogue ap malicious summary, on page 1768

- show rogue ap summary, on page 1770
- show rogue ap unclassified summary, on page 1773
- show rogue auto-contain, on page 1774
- show rogue client detailed, on page 1775
- show rogue client summary, on page 1776
- show rogue ignore-list, on page 1777
- show rogue rule detailed, on page 1779
- show rogue rule summary, on page 1781
- show route kernel, on page 1782
- show route summary, on page 1783
- show rules, on page 1784
- show run-config, on page 1785
- show run-config startup-commands , on page 1786
- show serial, on page 1787
- show sessions, on page 1788
- show snmpcommunity, on page 1789
- show snmpengineID, on page 1790
- show snmptrap, on page 1791
- show snmpv3user, on page 1792
- show snmpversion, on page 1793
- show spanningtree port, on page 1794
- show spanningtree switch, on page 1795
- show stats port, on page 1796
- show stats switch, on page 1798
- show switchconfig, on page 1800
- show sysinfo, on page 1801
- show tacacs acct statistics, on page 1803
- show tacacs auth statistics, on page 1804
- show tacacs summary, on page 1805
- show tech-support, on page 1806
- show time, on page 1807
- show trapflags, on page 1809
- show traplog, on page 1811
- show tunnel profile summary, on page 1812
- show tunnel profile-detail, on page 1813
- show tunnel eogre-summary, on page 1814
- show tunnel eogre-statistics, on page 1815
- show tunnel eogre-domain-summary, on page 1816
- show tunnel eogre gateway, on page 1817
- show watchlist, on page 1818
- show wlan, on page 1819
- show wps ap-authentication summary, on page 1824
- show wps cids-sensor, on page 1825
- show wps mfp, on page 1826
- show wps shun-list, on page 1827
- show wps signature detail, on page 1828

- show wps signature events, on page 1829
- show wps signature summary, on page 1831
- show wps summary, on page 1833
- show wps wips statistics, on page 1835
- show wps wips summary, on page 1836
- show wps ap-authentication summary, on page 1837

show radius acct detailed

To display RADIUS accounting server information, use the **show radius acct detailed** command.

show radius acct detailed *radius_index*

Syntax Description

radius_index	Radius server index. The range is from 1 to 17.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to display RADIUS accounting server information:

```
(Cisco Controller) > show radius acct detailed 5

Radius Index........5
NAI Realms..........LAB.VTV.BLR.cisco.co.in
```

show radius acct statistics

To display the RADIUS accounting server statistics for the Cisco wireless LAN controller, use the **show radius acct statistics** command.

show radius acct statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display RADIUS accounting server statistics:

```
(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
```

Related Commands

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

To display RADIUS authentication server information, use the **show radius auth detailed** command.

show radius auth detailed *radius_index*

Syntax Description

radius_index	Radius server index. The range is from 1 to 17.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to display RADIUS authentication server information:

```
(Cisco Controller) > show radius auth detailed 1

Radius Index.....1
NAI Realms.....LAB.VTV.BLR.cisco.co.in
```

show radius auth statistics

To display the RADIUS authentication server statistics for the Cisco wireless LAN controller, use the **show radius auth statistics** command.

show radius auth statistics

This command has no arguments or keyword.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display RADIUS authentication server statistics:

```
(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
```

Related Commands

config radius auth

config radius auth management

config radius auth network

show radius summary

show radius avp-list

To display RADIUS VSA AVPs, use the **show radius avp-list** command.

show radius avp-list *profile-name*

Syntax Description

profile-name	Profile name for which downloaded AVPs to be shown.

Command Default

None

Command History

Release	Modification
8.0	This command was introduced.

The following example shows how to display RADIUS VSA AVPs:

```
(Cisco Controller) > show radius avp-list
```

show radius summary

To display the RADIUS authentication and accounting server summary, use the **show radius summary** command.

show radius summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a RADIUS authentication server summary:

```
(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
-----  ----  ---------------  ------  --------  ----  --------  --------------
--------------------------------
```

Related Commands

show radius auth statistics

show radius acct statistics

show redundancy interfaces

To display details of redundancy and service port IP addresses, use the **show redundancy interfaces** command.

show redundancy interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the redundancy and service port IP addresses information:

```
(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

To display the average latency to reach the management gateway and the peer redundancy management IP address, use the **show redundancy latency** command .

show redundancy latency

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the average latency to reach the management gateway and the peer redundancy management IP address:

```
(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

To display the High Availability (HA) mobility MAC address that is used to communicate with the peer, use the **show redundancy mobilitymac** command.

show redundancy mobilitymac

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the HA mobility MAC address used to communicate with the peer:

```
(Cisco Controller) >show redundancy mobilitymac
          ff:ff:ff:ff:ff:ff
```

show redundancy peer-route summary

To see the routes assigned to the standby controller, use the **show redundancy peer-route summary** command.

show redundancy peer-route summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to view all the configured routes of the standby controller:

```
(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

To see statistical information about the standby controller, use the **show redundancy peer-system statistics** command.

show redundancy peer-system statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
8.7	The serial number and fan status of the standby controller are added to the output of the command.
7.6	This command was introduced in a release earlier than Release 7.6.

```
(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

To display the statistics information of the Redundancy Manager, use the **show redundancy statistics** command.

show redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command displays the statistics of different redundancy counters.

Local Physical Ports - Connectivity status of each physical port of the controller. 1 indicates that the port is up and 0 indicates that the port is down.

Peer Physical Ports - Connectivity status of each physical port of the peer controller. 1 indicates that the port is up and 0 indicates that the port is down.

The following example shows how to display the statistics information of the Redundancy Manager:

```
(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

To display the redundancy summary information, use the **show redundancy summary** command.

show redundancy summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the redundancy summary information of the controller:

```
(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

To display details of the Redundancy Manager timers, use the **show redundancy timers** command.

show redundancy timers

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the details of the Redundancy Manager timers:

```
(Cisco Controller) >show redundancy timers

          Keep Alive Timer         : 100 msecs

          Peer Search Timer        : 120 secs
```

show remote-lan

To display information about remote LAN configuration, use the **show remote-lan** command.

show remote-lan { **summary** | *remote-lan-id* }

Syntax Description

summary	Displays a summary of all remote LANs.
remote-lan-id	Remote LAN identifier.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all remote LANs:

```
(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
```

The following example shows configuration information about the remote LAN with the *remote-lan-id* 2:

```
(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

To display the scheduled system reset parameters, use the **show reset** command.

show reset

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the scheduled system reset parameters:

```
> 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.
```

Related Commands

reset system at

reset system in

reset system cancel

reset system notify-time

show rfid client

To display the radio frequency identification (RFID) tags that are associated to the controller as clients, use the **show rfid client** command.

show rfid client

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Usage Guidelines

When the RFID tag is not in client mode, the above fields are blank.

This example shows how to display the RFID tag that is associated to the controller as clients:

```
> 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
```

Related Commands

config rfid status

config rfid timeout

show rfid config

show rfid detail

show rfid summary

show rfid config

To display the current radio frequency identification (RFID) configuration settings, use the **show rfid config** command.

show rfid config

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the current RFID configuration settings:

```
> show rfid config
RFID Tag Data Collection ............................. Enabled
RFID Tag Auto-Timeout ................................ Enabled
RFID Client Data Collection .......................... Disabled
RFID Data Timeout .................................... 200 seconds
```

Related Commands

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid summary

show rfid detail

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show rfid detail** command.

show rfid detail *mac_address*

Syntax Description

mac_address	MAC address of an RFID tag.

Command Default

None.

This example shows how to display detailed RFID information:

```
> 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
```

Related Commands

config rfid status

config rfid timeout

show rfid config

show rfid client

show rfid summary

show rfid summary

To display a summary of the radio frequency identification (RFID) information for a specified tag, use the **show rfid summary** command.

show rfid summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display a summary of RFID information:

```
> 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
```

Related Commands

config rfid status

config rfid timeout

show rfid client

show rfid detail

show rfid config

show rf-profile summary

To display a summary of RF profiles in the controller, use the **show rf-profile summary** command.

show rf-profile summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is the output of the **show rf-profile summary** command:

```
(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

To display the RF profile details in the Cisco wireless LAN controller, use the **show rf-profile details** command.

show rf-profile details *rf-profile-name*

Syntax Description

rf-profile-name	Name of the RF profile.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The output was updated to include the Rx SOP threshold.
8.5	The output was updated to include the Client Aware FRA configurations.

The following is the output of the **show rf-profile details** command::

```
(Cisco Controller) >show rf-profile details profile1
Description..................................... <none>
AP Group Name................................... test
Radio policy.................................... 5 GHz
11n-client-only................................. disabled
Transmit Power Threshold v1..................... -70 dBm
Transmit Power Threshold v2..................... -67 dBm
Min Transmit Power.............................. -10 dBm
Max Transmit Power.............................. 30 dBm
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

WLAN ID          Max Clients
-------          -------
  1                600

--More-- or (q)uit
  2                600
  4                600
  9                600
  11               600
  12               600
  13               600
  14               600
  15               600
  16               600
```

```
Trap Threshold
    Clients..................................... 12 clients
    Interference................................ 10 %
    Noise....................................... -70 dBm
    Utilization................................. 80 %
Multicast Data Rate............................. 0
Rx Sop Threshold................................ AUTO
Cca Threshold................................... 0 dBm
Slot Admin State:............................... Enabled

Client Aware FRA
    State....................................... Disabled
    Client Select Utilization Threshold.......... 20%

--More-- or (q)uit
    Client Reset Utilization Threshold........... 5%

Band Select
    Probe Response.............................. Disabled
    Cycle Count................................. 2 cycles
    Cycle Threshold............................. 200 milliseconds
    Expire Suppression.......................... 20 seconds
    Expire Dual Band............................ 60 seconds
    Client Rssi................................. -80 dBm
    Client Mid Rssi............................. -80 dBm

Load Balancing
    Denial...................................... 3 count
    Window...................................... 5 clients

Coverage Data
    Data........................................ -80 dBm
    Voice....................................... -80 dBm
    Minimum Client Level........................ 3 clients
    Exception Level............................. 25 %
DCA Channel List................................ 36,40,44,48,52,56,60,64,100,
                                                 104,108,112,116,120,124,128,
                                                 132,136,140,144,149,153,157,

--More-- or (q)uit
                                                 161
DCA Bandwidth................................... 20
DCA Foreign AP Contribution..................... enabled
HSR Mode........................................ disabled

802.11n MCS Rates
    MCS-00 Rate................................. enabled
    MCS-01 Rate................................. enabled
    MCS-02 Rate................................. enabled
    MCS-03 Rate................................. enabled
    MCS-04 Rate................................. enabled
    MCS-05 Rate................................. enabled
    MCS-06 Rate................................. enabled
    MCS-07 Rate................................. enabled
    MCS-08 Rate................................. enabled
    MCS-09 Rate................................. enabled
    MCS-10 Rate................................. enabled
    MCS-11 Rate................................. enabled
    MCS-12 Rate................................. enabled
    MCS-13 Rate................................. enabled
    MCS-14 Rate................................. enabled
    MCS-15 Rate................................. enabled
    MCS-16 Rate................................. enabled
```

```
--More-- or (q)uit
    MCS-17 Rate..................................... enabled
    MCS-18 Rate..................................... enabled
    MCS-19 Rate..................................... enabled
    MCS-20 Rate..................................... enabled
    MCS-21 Rate..................................... enabled
    MCS-22 Rate..................................... enabled
    MCS-23 Rate..................................... enabled
    MCS-24 Rate..................................... enabled
    MCS-25 Rate..................................... enabled
    MCS-26 Rate..................................... enabled
    MCS-27 Rate..................................... enabled
    MCS-28 Rate..................................... enabled
    MCS-29 Rate..................................... enabled
    MCS-30 Rate..................................... enabled
    MCS-31 Rate..................................... enabled
 Client Network Preference.......................... default
```

show rogue adhoc custom summary

To display information about custom rogue ad-hoc rogue access points, use the **show rogue adhoc custom summary** command.

show rogue adhoc custom summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc custom summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

Related Commands

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

To display details of an ad-hoc rogue access point detected by the Cisco wireless LAN controller, use the **show rogue adhoc client detailed** command.

show rogue adhoc detailed *MAC_address*

Syntax Description

MAC_address	Adhoc rogue MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed ad-hoc rogue MAC address information:

```
(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
```

Related Commands

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

To display information about friendly rogue ad-hoc rogue access points, use the **show rogue adhoc friendly summary** command.

show rogue adhoc friendly summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about friendly rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc friendly summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

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

To display information about malicious rogue ad-hoc rogue access points, use the **show rogue adhoc malicious summary** command.

show rogue adhoc malicious summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display details of malicious rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc malicious summary
Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------ -----  ---------
-----------------------
```

Related Commands

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

To display information about unclassified rogue ad-hoc rogue access points, use the **show rogue adhoc unclassified summary** command.

show rogue adhoc unclassified summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about unclassified rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue adhoc unclassified summary

Number of Adhocs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

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

To display a summary of the ad-hoc rogue access points detected by the Cisco wireless LAN controller, use the **show rogue adhoc summary** command.

show rogue adhoc summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all ad-hoc rogues:

```
(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
```

Related Commands

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

To display details of rogue access point clients detected by the Cisco wireless LAN controller, use the **show rogue ap clients** command.

show rogue ap clients *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display details of rogue access point clients:

```
(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
```

Related Commands

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

To display information about custom rogue ad-hoc rogue access points, use the **show rogue ap custom summary** command.

show rogue ap custom summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display details of custom rogue ad-hoc rogue access points:

```
(Cisco Controller) > show rogue ap custom summary

Number of APs.............................0

MAC Address        State               # APs # Clients Last Heard
-----------------  ------------------- ----- ---------
-----------------------
```

Related Commands

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

To display details of a rogue access point detected by the Cisco wireless LAN controller, use the **show rogue-ap detailed** command.

show rogue ap detailed *ap_mac_address*

Syntax Description

ap_mac_address	Rogue access point MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed information of a rogue access point:

```
(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
```

This example shows how to display detailed information of a rogue access point with a customized classification:

```
(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
```

Related Commands

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

To display a list of the friendly rogue access points detected by the controller, use the **show rogue ap friendly summary** command.

show rogue ap friendly summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all friendly rogue access points:

```
(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
```

Related Commands

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

To display a list of the malicious rogue access points detected by the controller, use the **show rogue ap malicious summary** command.

show rogue ap malicious summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all malicious rogue access points:

```
(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
```

Related Commands

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

To display a summary of the rogue access points detected by the Cisco wireless LAN controller, use the **show rogue-ap summary** command.

show rogue ap summary{**ssid** | **channel**}

Syntax Description

ssid	Displays specific user-configured SSID of the rogue access point.
channel	Displays specific user-configured radio type and channel of the rogue access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The new keywords **SSID** and **channel** are added.

The following example shows how to display a summary of all rogue access points:

```
(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
```

The following example shows how to display a summary of all rogue access points with SSID as extended parameter.

```
(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
```

The following example shows how to display a summary of all rogue access points with channel as extended parameter.

```
(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
```

The following example shows how to display a summary of all rogue access points with both SSID and channel as extended parameters.

```
(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
```

Related Commands

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

To display a list of the unclassified rogue access points detected by the controller, use the **show rogue ap unclassified summary** command.

show rogue ap unclassified summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a list of all unclassified rogue access points:

```
(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

To display information about rogue auto-containment, use the **show rogue auto-contain** command.

show rogue auto-contain

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display information about rogue auto-containment:

```
(Cisco Controller) > show rogue auto-contain
Containment Level.............................. 3
monitor_ap_only................................ false
```

Related Commands

config rogue adhoc

config rogue auto-contain level

show rogue client detailed

To display details of a rogue client detected by a Cisco wireless LAN controller, use the **show rogue client detailed** command.

show rogue client detailed *Rogue_AP MAC_address*

Syntax Description

Rogue_AP	Rogue AP address.
MAC_address	Rogue client MAC address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.1	The *Rogue_AP* parameter to the **show rogue client detailed** command is added.

The following example shows how to display detailed information for a rogue client:

```
(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
```

Related Commands

show rogue client summary

show rogue ignore-list

config rogue rule client

config rogue rule

show rogue client summary

To display a summary of the rogue clients detected by the Cisco wireless LAN controller, use the **show rogue client summary** command.

show rogue client summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a list of all rogue clients:

```
(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
```

Related Commands

show rogue client detailed

show rogue ignore-list

config rogue client

config rogue rule

show rogue ignore-list

To display a list of rogue access points that are configured to be ignored, use the **show rogue ignore-list** command.

show rogue ignore-list

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a list of all rogue access points that are configured to be ignored.

```
(Cisco Controller) > show rogue ignore-list

MAC Address
-----------------
xx:xx:xx:xx:xx:xx
```

Related Commands

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

To display detailed information for a specific rogue classification rule, use the **show rogue rule detailed** command.

show rogue rule detailed *rule_name*

Syntax Description

rule_name	Rogue rule name.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed information on a specific rogue classification rule:

```
(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
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule summary

show rogue rule summary

To display the rogue classification rules that are configured on the controller, use the **show rogue rule summary** command.

show rogue rule summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(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
```

The following example shows how to display a list of all rogue rules that are configured on the controller:

```
(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
```

Related Commands

config rogue rule

show rogue ignore-list

show rogue rule detailed

show route kernel

To display the kernel route cache information, use the **show route kernel** command.

show route kernel

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the kernel route cache information:

```
> 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
```

Related Commands

clear ap

debug arp

show arp kernel

config route add

config route delete

show route summary

To display the routes assigned to the Cisco wireless LAN controller service port, use the **show route summary** command.

show route summary

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display all the configured routes:

```
> show route summary
Number of Routes.............................. 1
Destination Network          Genmask              Gateway
-------------------    -------------------   -------------------
xxx.xxx.xxx.xxx        255.255.255.0         xxx.xxx.xxx.xxx
```

Related Commands

config route

show rules

To display the active internal firewall rules, use the **show rules** command.

show rules

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display active internal firewall rules:

```
(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

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the **show run-config all** command.

show run-config {**all** | **commands**} [**no-ap** | **commands**]

Syntax Description

all	Shows all the commands under the show run-config.
no-ap	(Optional) Excludes access point configuration settings.
commands	(Optional) Displays a list of user-configured commands on

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.2	This command was introduced .

Usage Guidelines

These commands have replaced the **show running-config** command.

Some WLAN controllers may have no Crypto Accelerator (VPN termination module) or power supplies listed because they have no provisions for VPN termination modules or power supplies.

The **show run-config all** command shows only values configured by the user. It does not show system-configured default values.

The following is a sample output of the **show run-config all** command:

```
(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

To display a comprehensive view of the current Cisco wireless LAN controller configuration, use the **showrun-configstartup-commands** command.

show run-configstartup-commands

Syntax Description

run-config	Displays the running configuration commands.
startup-commands	Display list of configured startup commands on Wireless LAN Controller.

Command Default

None

Command History

Release	Modification
8.0	

Usage Guidelines

The configuration commands on the Wireless LAN controller are uploaded to the TFTP or NCS servers using the transfer upload process. The **show run-config startup-commands** command enables the Wireless LAN controller to generate running-configuration in CLI format. The configuration commands generated can be used as backup configuration to restore the network.

Example

The following is a sample output of the **show run-config startup-commands** command:

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

To display the serial (console) port configuration, use the **show serial** command.

show serial

Syntax Description

This command has no arguments or keywords.

Command Default

The default values for Baud rate, Character, Flow Control, Stop Bits, Parity type of the port configuration are 9600, 8, off, 1, none.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display EIA-232 parameters and the serial port inactivity timeout:

```
(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

To display the console port login timeout and maximum number of simultaneous command-line interface (CLI) sessions, use the **show sessions** command.

show sessions

Syntax Description

This command has no arguments or keywords.

Command Default

5 minutes, 5 sessions.

This example shows how to display the CLI session configuration setting:

```
> show sessions
CLI Login Timeout (minutes)..... 0
Maximum Number of CLI Sessions..... 5
```

The response indicates that the CLI sessions never time out and that the Cisco wireless LAN controller can host up to five simultaneous CLI sessions.

Related Commands

config sessions maxsessions

config sessions timeout

show snmpcommunity

To display Simple Network Management Protocol (SNMP) community entries, use the **show snmpcommunity** command.

show snmpcommunity

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP community entries:

```
> 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
```

Related Commands

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

To display the SNMP engine ID, use the **show snmpengineID** command.

show snmpengineID

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the SNMP engine ID:

```
> show snmpengineID
SNMP EngineId... ffffffffffff
```

Related Commands

config snmp engineID

show snmptrap

To display Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap receivers and their status, use the **show snmptrap** command.

show snmptrap

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP trap receivers and their status:

```
> show snmptrap
SNMP Trap Receiver Name    IP Address        Status
-----------------------    ----------------- --------
xxx.xxx.xxx.xxx            xxx.xxx.xxx.xxx   Enable
```

show snmpv3user

To display Simple Network Management Protocol (SNMP) version 3 configuration, use the **show snmpv3user** command.

show snmpv3user

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display SNMP version 3 configuration information:

```
> show snmpv3user
SNMP v3 username    AccessMode  Authentication Encryption
------------------- ----------- -------------- ----------
default              Read/Write  HMAC-SHA       CFB-AES
```

Related Commands

config snmp v3user create

config snmp v3user delete

show snmpversion

To display which versions of Simple Network Management Protocol (SNMP) are enabled or disabled on your controller, use the **show snmpversion** command.

show snmpversion

Syntax Description

This command has no arguments or keywords.

Command Default

Enable.

This example shows how to display the SNMP v1/v2/v3 status:

```
> show snmpversion
SNMP v1  Mode..................................... Disable
SNMP v2c Mode..................................... Enable
SNMP v3  Mode..................................... Enable
```

Related Commands

config snmp version

show spanningtree port

To display the Cisco wireless LAN controller spanning tree port configuration, use the **show spanningtree port** command.

show spanningtree port *port*

Syntax Description

port	Physical port number: • 1 through 4 on Cisco 2100 Series Wireless LAN Controller. • 1 or 2 on Cisco 4402 Series Wireless LAN Controller. • 1 through 4 on Cisco 4404 Series Wireless LAN Controller.

Command Default

The default SPT configuration output values are 800C, Disabled, 802.1D, 128, 100, Auto.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When the a Cisco 4400 Series wireless LAN controller is configured for port redundancy, the Spanning Tree Protocol (STP) must be disabled for all ports on the Cisco 4400 Series Wireless LAN Controller. STP can remain enabled on the switch connected to the Cisco 4400 Series Wireless LAN Controller.

Note Some WLAN controllers do not support the spanning tree function.

The following example shows how to display spanning tree values on a per port basis:

```
(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

To display the Cisco wireless LAN controller network (DS port) spanning tree configuration, use the **show spanningtree switch** command.

show spanningtree switch

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

Some WLAN controllers do not support the spanning tree function.

The following example shows how to display spanning tree values on a per switch basis:

```
(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

To display physical port receive and transmit statistics, use the **show stats port** command.

show stats port {**detailed** *port* | **summary** *port*}

Syntax Description

detailed	Displays detailed port statistics.
summary	Displays port summary statistics.
port	Physical port number: • 1 through 4 on Cisco 2100 Series Wireless LAN Controllers. • 1 or 2 on Cisco 4402 Series Wireless LAN Controllers. • 1 through 4 on Cisco 4404 Series Wireless LAN Controllers. • 1 on Cisco WLCM Series Wireless LAN Controllers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the port summary information:

```
(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
```

The following example shows how to display the detailed port information:

```
(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

To display the network (DS port) receive and transmit statistics, use the **show stats switch** command.

show stats switch {**detailed** | **summary**}

Syntax Description

detailed	Displays detailed switch statistics.
summary	Displays switch summary statistics.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display switch summary statistics:

```
(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
```

The following example shows how to display detailed switch statistics:

```
(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

To display parameters that apply to the Cisco wireless LAN controller, use the **show switchconfig** command.

show switchconfig

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display parameters that apply to the Cisco wireless LAN controller:

```
(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
```

Related Commands

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig strong-pwd

config switchconfig flowcontrol

config switchconfig fips-prerequisite

show stats switch

show sysinfo

To see high-level controller information, use the **show sysinfo** command.

show sysinfo

Syntax Description

This command has no arguments or keywords.

Command Default

None

This example shows a sample output of the command run on Cisco 8540 Wireless Controller using Release 8.3:

```
 (Cisco Controller) >show sysinfo

Manufacturer's Name.............................. Cisco Systems Inc.
Product Name..................................... Cisco Controller
Product Version.................................. 8.3.100.0
RTOS Version..................................... 8.3.100.0
Bootloader Version............................... 8.0.110.0
Emergency Image Version.......................... 8.0.110.0

OUI File Last Update Time........................ Sun Sep 07 10:44:07 IST 2014


Build Type....................................... DATA + WPS

System Name...................................... TestSpartan8500Dev1
System Location.................................
System Contact..................................
System ObjectID.................................. 1.3.6.1.4.1.9.1.1615
Redundancy Mode.................................. Disabled
IP Address....................................... 8.1.4.2
IPv6 Address..................................... ::
System Up Time................................... 0 days 17 hrs 20 mins 58 secs

--More-- or (q)uit
System Timezone Location........................
System Stats Realtime Interval................... 5
System Stats Normal Interval..................... 180

Configured Country............................... Multiple Countries : IN,US
Operating Environment............................ Commercial (10 to 35 C)
Internal Temp Alarm Limits....................... 10 to 38 C
Internal Temperature............................. +21 C
Fan Status....................................... OK

RAID Volume Status
Drive 0.......................................... Good
Drive 1.......................................... Good

State of 802.11b Network......................... Enabled
State of 802.11a Network......................... Enabled
Number of WLANs.................................. 7
Number of Active Clients......................... 1

OUI Classification Failure Count................. 0

Burned-in MAC Address............................ F4:CF:E2:0A:27:00
```

```
Power Supply 1................................. Present, OK

--More-- or (q)uit
Power Supply 2................................. Present, OK
Maximum number of APs supported................ 6000
System Nas-Id.................................
WLC MIC Certificate Types...................... SHA1/SHA2
Licensing Type................................. RTU
```

show tacacs acct statistics

To display detailed radio frequency identification (RFID) information for a specified tag, use the **show tacacs acct statistics** command.

show tacacs acct statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display detailed RFID information:

```
(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 auth statistics

To display TACACS+ server authentication statistics, use the **show tacacs auth statistics** command.

show tacacs auth statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display TACACS server authentication statistics:

```
(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

To display TACACS+ server summary information, use the **show tacacs summary** command.

show tacacs summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display TACACS server summary information:

```
(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
...
```

Related Commands

config tacacs acct

config tacacs athr

config tacacs auth

show tacacs summary

show tacacs athr statistics

show tacacs auth statistics

show tech-support

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support** command.

show tech-support

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display system resource information:

```
> 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

To display the Cisco wireless LAN controller time and date, use the **show time** command.

show time

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display the controller time and date when authentication is not enabled:

```
> 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
```

This example shows successful authentication of NTP Message results in the AUTH Success:

```
> 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
```

This example shows that if the packet received has errors, then the NTP Msg Auth status will show AUTH Failure:

```
> 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
```

This example shows that if there is no response from NTP server for the packets, the NTP Msg Auth status will be blank:

```
> 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
```

Related Commands

config time manual

config time ntp

config time timezone

config time timezone location

show trapflags

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap flags, use the **show trapflags** command.

show trapflags

Syntax Description

This command has no arguments or keywords.

Command Default

None.

This example shows how to display controller SNMP trap flags:

```
> 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
```

Related Commands

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

To display the Cisco wireless LAN controller Simple Network Management Protocol (SNMP) trap log, use the **show traplog** command.

show traplog

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following is a sample output of the **show traplog** command:

```
(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

To show the summary of all the profiles, use the **show tunnel profile** command.

show tunnel profile { *summary* | *detail* { **<profile-name>** *profile-name* }

Syntax Description

summary	Summary of all profiles.
detail	Shows details of a specific profile.
profile-name	Name of the profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to display the summary of all the profiles:

```
show tunnel profile summary
```

show tunnel profile-detail

To show details of a specific profile, use the **show tunnel profile** command.

show tunnel profiledetail*profile-name*

Syntax Description

detail	Displays details of a specific profile.
profile-name	Name of the profile.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to display specific profile details:

```
show tunnel profile detail test
```

show tunnel eogre-summary

To show the global configuration summary, use the **show tunnel eogre** command.

show tunnel eogre summary

Syntax Description

summary	Displays the global configuration summary.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to display the global configuration details:

```
(Cisco Controller) > show tunnel eogre summary
```

show tunnel eogre-statistics

To display the EoGRE Tunnel statistics, use the **show tunnel eogre** command.

show tunnel eogrestatistics

Syntax Description

statistics	Displays the EoGRE Tunnel statistics.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to display the EoGRE Tunnel statistics details:

```
show tunnel eogre statistics
```

show tunnel eogre-domain-summary

To display the EoGRE domain summary, use the **show tunnel eogre** command.

show tunnel eogredomainsummary

Syntax Description

summary	Displays the EoGRE domain summary.

Command Default

None

Command History

Release	Modification
8.1	This command was introduced.

The following example shows how to display the EoGRE domain summary:

```
show tunnel eogre domain summary
```

show tunnel eogre gateway

To view the EoGRE tunnel gateway summary and statistics, use the **show tunnel eogre** command.

show tunnel eogre gateway {**summary** | **statistics**}

Syntax Description

summary	Displays the EoGRE tunnel gateway summary.
statistics	Displays the EoGRE tunnel gateway statistics.

Command Default

None

Usage Guidelines

The **show tunnel eogre gateway summary** command lists details of only the FlexConnect central switching clients and Local Mode AP clients. To view the details of FlexConnect local switching clients, use the **show ap eogre gateway** *ap-name* command.

Command History

Release	Modification
8.1	This command was introduced.
8.5	The **statistics** parameter was added.

show watchlist

To display the client watchlist, use the **show watchlist** command.

show watchlist

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the client watchlist information:

```
(Cisco Controller) >show watchlist
client watchlist state is disabled
```

show wlan

To display configuration information for a specified wireless LAN or a foreign access point, or to display wireless LAN summary information, use the **show wlan** command.

show wlan { **apgroups** | **summary** | *wlan_id* | **foreignAp** | **lobby-admin-access** }

Syntax Description

apgroups	Displays access point group information.
summary	Displays a summary of all wireless LANs.
wlan_id	Displays the configuration of a WLAN. The Wireless LAN id to 512.
foreignAp	Displays the configuration for support of foreign access point
lobby-admin-access	Display all wlans that have lobby-admin-access enabled.

Command Default

None

Usage Guidelines

For 802.1X client security type, which creates the PMK cache, the maximum session timeout that can be set is 86400 seconds when the session timeout is disabled. For other client security such as open, WebAuth, and PSK for which the PMK cache is not created, the session timeout value is shown as infinite when session timeout is disabled.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.4	Shows WLANs which have lobby-admin-access enabled.

The following example shows how to display a summary of wireless LANs for wlan_id 1:

```
(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
```

The following example shows how to display a summary of all WLANs:

```
(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
```

The following example shows how to display the configuration for support of foreign access points:

```
(Cisco Controller) >show wlan foreignap
```

```
Foreign AP support is not enabled.
```

The following example shows how to display the AP groups:

```
(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

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

Related Commands

config wps ap-authentication

show wps cids-sensor

To display Intrusion Detection System (IDS) sensor summary information or detailed information on a specified Wireless Protection System (WPS) IDS sensor, use the **show wps cids-sensor** command.

show wps cids-sensor {**summary** | **detail** *index*}

Syntax Description

summary	Displays a summary of sensor settings.
detail	Displays all settings for the selected sensor.
index	IDS sensor identifier.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display all settings for the selected sensor:

```
(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
```

Related Commands

config wps ap-authentication

show wps mfp

To display Management Frame Protection (MFP) information, use the **show wps mfp** command.

show wps mfp {**summary** | **statistics**}

Syntax Description

summary	Displays the MFP configuration and status.
statistics	Displays MFP statistics.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the MFP configuration and status:

```
(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
```

The following example shows how to display the MFP statistics:

```
(Cisco Controller) > show wps mfp statistics
BSSID             Radio Validator AP         Last Source Addr  Found  Error Type
     Count      Frame Types
----------------- ----- -------------------- ----------------- ------ ----------
---- ---------- -----------
no errors
```

Related Commands

config wps mfp

show wps shun-list

To display the Intrusion Detection System (IDS) sensor shun list, use the **show wps shun-list** command.

show wps shun-list

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the IDS system sensor shun list:

```
(Cisco Controller) > show wps shun-list
```

Related Commands

config wps shun-list re-sync

show wps signature detail

To display installed signatures, use the **show wps signature detail** command.

show wps signature detail *sig-id*

Syntax Description

sig-id	Signature ID of an installed signature.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

This example shows how to display information on the attacks detected by standard signature 1:

```
(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
```

Related Commands

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

To display more information about the attacks detected by a particular standard or custom signature, use the **show wps signature events** command.

show wps signature events {**summary** | {**standard** | **custom**} *precedenceID* {**summary** | **detailed**}

Syntax Description

summary	Displays all tracking signature summary information.
standard	Displays Standard Intrusion Detection System (IDS) signature settings.
custom	Displays custom IDS signature settings.
precedenceID	Signature precedence identification value.
detailed	Displays tracking source MAC address details.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the number of attacks detected by all enabled signatures:

```
(Cisco Controller) > show wps signature events summary
Precedence  Signature Name        Type       # Events
----------  --------------------  --------   --------
1           Bcast deauth          Standard      2
2           NULL probe resp 1     Standard      1
```

This example shows how to display a summary of information on the attacks detected by standard signature 1:

```
(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
```

Related Commands

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

To see individual summaries of all of the standard and custom signatures installed on the controller, use the **show wps signature summary** command.

show wps signature summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of all of the standard and custom signatures:

```
(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
...
```

Related Commands

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

To display Wireless Protection System (WPS) summary information, use the **show wps summary** command.

show wps summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display WPS summary information:

```
(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
...
```

Related Commands

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

To display the current state of the Cisco Wireless Intrusion Prevention System (wIPS) operation on the controller, use the **show wps wips statistics** command.

show wps wips statistics

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display the statistics of the wIPS operation:

```
(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
```

Related Commands

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

To display the adaptive Cisco Wireless Intrusion Prevention System (wIPS) configuration that the Wireless Control System (WCS) forwards to the controller, use the **show wps wips summary** command.

show wps wips summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the wIPS configuration:

```
(Cisco Controller) > show wps wips summary
Policy Name..................................... Default
Policy Version.................................. 3
```

Related Commands

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

To display the access point neighbor authentication configuration on the controller, use the **show wps ap-authentication summary** command.

show wps ap-authentication summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to display a summary of the Wireless Protection System (WPS) access point neighbor authentication:

```
(Cisco Controller) > show wps ap-authentication summary
AP neighbor authentication is <disabled>.
Authentication alarm threshold is 1.
RF-Network Name: <B1>
```

Related Commands

config wps ap-authentication

PART VIII

Miscellaneous Commands

- Miscellaneous Commands: 1, on page 1841
- Miscellaneous Commands: 2, on page 1847

Miscellaneous Commands: 1

- cping, on page 1842
- eping, on page 1843
- mping, on page 1844
- ping, on page 1845

cping

To test mobility data traffic using CAPWAP, use the **cping** command.

cping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address	IP address of a peer mobility controller.

Command Default

None

Command History

Release	Modification
7.5	This command was introduced in the controller 7.5 Release.

Usage Guidelines

This command tests the mobility data traffic using the new mobility architecture.

The following example shows how to test the data traffic of a controller with peer mobility IP address as 172.12.35.31:

```
(Cisco Controller) >cping 172.12.35.31
```

eping

To test the mobility Ethernet over IP (EoIP) data packet communication between two controllers, use the **eping** command.

eping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address	IP address of a controller that belongs to a mobility group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command tests the mobility data traffic over the management interface.

Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

The IPv6 address format for this command is not supported.

The following example shows how to test EoIP data packets and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
(Cisco Controller) >eping 172.12.35.31
```

mping

To test mobility UDP control packet communication between two controllers, use the **mping** command.

mping *mobility_peer_IP_address*

Syntax Description

mobility_peer_IP_address	IP address of a controller that belongs to a mobility group.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

Usage Guidelines

This test runs over mobility UDP port 16666. It tests whether the mobility control packet can be reached over the management interface.

Note This ping test is not Internet Control Message Protocol (ICMP) based. The term “ping” is used to indicate an echo request and an echo reply message.

The following example shows how to test mobility UDP control packet communications and to set the IP address of a controller that belongs to a mobility group to 172.12.35.31:

```
(Cisco Controller) >mping 172.12.35.31
```

ping

To send ICMP echo packets to a specified IP address, use the ping command:

ping *ip-addr* *interface-name*

Syntax Description

ip-addr	IP address of the interface that you are trying to send ICMP echo packets to
interface-name	Name of the interface to which you are trying to send ICMP echo packets

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

When you run the **ping** command, the CPU spikes up to 98 percent in the “osapi_ping_rx process”. While the **ping** command is running, the terminal and web activity on the controller is blocked.

Example

The following example shows how to send ICMP echo packets to an interface:

```
(Cisco Controller) >ping 209.165.200.225 dyn-interface-1
```

Miscellaneous Commands: 2

- capwap ap controller ip address, on page 1849
- config ap dhcp release-override, on page 1850
- capwap ap dot1x, on page 1851
- capwap ap hostname, on page 1852
- capwap ap ip address, on page 1853
- capwap ap ip default-gateway, on page 1854
- capwap ap log-server, on page 1855
- capwap ap primary-base, on page 1856
- capwap ap primed-timer, on page 1857
- capwap ap secondary-base, on page 1858
- capwap ap tertiary-base, on page 1859
- lwapp ap controller ip address, on page 1860
- reset system at, on page 1861
- reset system in, on page 1862
- reset system cancel, on page 1863
- reset system notify-time, on page 1864
- reset peer-system, on page 1865
- save config, on page 1866
- transfer download certpasswor, on page 1867
- transfer download datatype, on page 1868
- transfer download datatype icon, on page 1869
- transfer download filename, on page 1870
- transfer download mode, on page 1871
- transfer download password, on page 1872
- transfer download path, on page 1873
- transfer download port, on page 1874
- transfer download serverip, on page 1875
- transfer download start, on page 1876
- transfer download tftpPktTimeout, on page 1877
- transfer download tftpMaxRetries, on page 1878
- transfer download username, on page 1879
- transfer encrypt, on page 1880
- transfer upload datatype, on page 1881

- transfer upload filename, on page 1883
- transfer upload mode, on page 1884
- transfer upload pac, on page 1885
- transfer upload password, on page 1886
- transfer upload path, on page 1887
- transfer upload peer-start, on page 1888
- transfer upload port, on page 1889
- transfer upload serverip, on page 1890
- transfer upload start, on page 1891
- transfer upload username, on page 1892

capwap ap controller ip address

To configure the controller IP address into the CAPWAP access point from the access point's console port, use the **capwap ap controller ip address** command.

capwap ap controller ip address *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases.

The following example shows how to configure the controller IP address 10.23.90.81 into the CAPWAP access point:

```
ap_console >capwap ap controller ip address 10.23.90.81
```

config ap dhcp release-override

To configure DHCP release override on Cisco APs, use the **config ap dhcp release-override** command.

config ap dhcp release-override {**enable** | **disable**} {*cisco-ap-name* | **all**}

Syntax Description

enable	Enables DHCP release override and sets number of DHCP releases sent by AP to 1. To be used as a workaround for a few DHCP servers that mark the AP's IP address as bad. We recommend that you use this configuration only in highly reliable networks.
disable	Disables DHCP release override and sets number of DHCP releases sent by AP to 3, which is the default value. This ensures that the DHCP server receives the release message even if one of the packets is lost.
cisco-ap-name	Configuration is applied to the Cisco AP that you enter
all	Configuration is applied to all Cisco APs

Command Default

Disabled

Command History

Release	Modification
8.2	This command was introduced.

Usage Guidelines

Use this command when you are using Cisco lightweight APs with Windows Server 2008 R2 or 2012 as the DHCP server.

capwap ap dot1x

To configure the dot1x username and password into the CAPWAP access point from the access point's console port, use the **capwap ap dot1x** command.

capwap ap dot1x username *user_name* **password** *password*

Syntax Description

user_name	Dot1x username.
password	Dot1x password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the dot1x username ABC and password pass01:

```
ap_console >capwap ap dot1x username ABC password pass01
```

capwap ap hostname

To configure the access point host name from the access point's console port, use the **capwap ap hostname** command.

capwap ap hostname *host_name*

Syntax Description

host_name	Hostname of the access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases. This command is available only for the Cisco Lightweight AP IOS Software recovery image (rcvk9w8) without any private-config. You can remove the private-config by using the **clear capwap private-config** command.

This example shows how to configure the hostname controller into the CAPWAP access point:

```
ap_console >capwap ap hostname controller
```

capwap ap ip address

To configure the IP address into the CAPWAP access point from the access point's console port, use the **capwap ap ip address** command.

capwap ap ip address *A.B.C.D*

Syntax Description

A.B.C.D	IP address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the IP address 10.0.0.1 into CAPWAP access point:

```
ap_console >capwap ap ip address 10.0.0.1
```

capwap ap ip default-gateway

To configure the default gateway from the access point's console port, use the **capwap ap ip default-gateway** command.

capwap ap ip default-gateway *A.B.C.D*

Syntax Description

A.B.C.D	Default gateway address of the capwap access point.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the CAPWAP access point with the default gateway address 10.0.0.1:

```
ap_console >capwap ap ip default-gateway 10.0.0.1
```

capwap ap log-server

To configure the system log server to log all the CAPWAP errors, use the **capwap ap log-server** command.

capwap ap log-server *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the syslog server.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the syslog server with the IP address 10.0.0.1:

```
ap_console >capwap ap log-server 10.0.0.1
```

capwap ap primary-base

To configure the primary controller name and IP address into the CAPWAP access point from the access point's console port, use the **capwap ap primary-base** command.

Note This command configures the IPv4 and IPv6 address for Cisco Wave 2 APs.

capwap ap primary-base *WORD A.B.C.D*

Syntax Description

WORD	Name of the primary controller.
A.B.C.D	IP address of the primary controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports IPv4 and IPv6 address format.

Usage Guidelines

This command must be entered from an access point's console port in enable mode (elevated access).

This example shows how to configure the primary controller name WLC1 and primary controller IP address 209.165.200.225 into the CAPWAP access point:

```
ap_console >capwap ap primary-base WLC1 209.165.200.225
```

capwap ap primed-timer

To configure the primed timer into the CAPWAP access point, use the **capwap ap primed-timer** command.

capwap ap primed-timer {**enable** | **disable**}

Syntax Description

enable	Enables the primed timer settings
disable	Disables the primed timer settings.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

This command must be entered from an access point's console port.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to enable the primed-timer settings:

```
ap_console >capwap ap primed-timer enable
```

capwap ap secondary-base

To configure the name and IP address of the secondary controller into the CAPWAP access point from the access point's console port, use the **capwap ap secondary-base** command.

capwap ap secondary-base *controller_name controller_ip_address*

Syntax Description

controller_name	Name of the secondary controller.
controller_ip_address	IP address of the secondary controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco Access Point IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the secondary controller name as WLC2 and secondary controller IP address 209.165.200.226 into the CAPWAP access point:

```
ap_console >capwap ap secondary-base WLC2 209.165.200.226
```

capwap ap tertiary-base

To configure the name and IP address of the tertiary controller into the CAPWAP access point from the access point's console port, use the **capwap ap tertiary-base** command.

capwap ap tertiary-base *WORDA.B.C.D*

Syntax Description

WORD	Name of the tertiary controller.
A.B.C.D	IP address of the tertiary controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command supports only IPv4 address format.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or later releases.

This example shows how to configure the tertiary controller with the name WLC3 and secondary controller IP address 209.165.200.227 into the CAPWAP access point:

```
ap_console >capwap ap tertiary-base WLC3 209.165.200.227
```

lwapp ap controller ip address

To configure the controller IP address into the FlexConnect access point from the access point's console port, use the **lwapp ap controller ip address** command.

lwapp ap controller ip address *A.B.C.D*

Syntax Description

A.B.C.D	IP address of the controller.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports only IPv4 address format.

Usage Guidelines

This command must be entered from an access point's console port. This command is applicable for IPv4 addresses only.

Prior to changing the FlexConnect configuration on an access point using the access point's console port, the access point must be in standalone mode (not connected to a controller) and you must remove the current LWAPP private configuration by using the **clear lwapp private-config** command.

Note The access point must be running Cisco IOS Release 12.3(11)JX1 or higher releases.

The following example shows how to configure the controller IP address 10.92.109.1 into the FlexConnect access point:

```
ap_console > lwapp ap controller ip address 10.92.109.1
```

reset system at

To reset the system at a specified time, use the **reset system at** command.

reset system at YYYY-MM-DD HH : MM : SS image {**no-swap** | **swap**} **reset-aps** [**save-config**]

Syntax Description

YYYY-MM-DD	Specifies the date.
HH: MM: SS	Specifies the time in a 24-hour format.
image	Configures the image to be rebooted.
swap	Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	(Optional) Saves the configuration before the system reset.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the system at 2010-03-29 and 12:01:01 time:

```
(Cisco Controller) > reset system at 2010-03-29 12:01:01 image swap reset-aps save-config
```

reset system in

To specify the amount of time delay before the devices reboot, use the **reset system in** command.

reset system in HH : MM : SS image {**swap** | **no-swap**} **reset-aps save-config**

Syntax Description

HH :MM :SS	Specifies a delay in duration.
image	Configures the image to be rebooted.
swap	Changes the active boot image; boots the non-active image and sets the default flag on it on the next reboot.
no-swap	Boots from the active image.
reset-aps	Resets all access points during the system reset.
save-config	Saves the configuration before the system reset.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the system after a delay of 00:01:01:

```
(Cisco Controller) > reset system in 00:01:01 image swap reset-aps save-config
```

reset system cancel

To cancel a scheduled reset, use the **reset system cancel** command.

reset system cancel

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to cancel a scheduled reset:

```
(Cisco Controller) > reset system cancel
```

reset system notify-time

To configure the trap generation prior to scheduled resets, use the **reset system notify-time** command.

reset system notify-time *minutes*

Syntax Description

minutes	Number of minutes before each scheduled reset at which to generate a trap.

Command Default

The default time period to configure the trap generation prior to scheduled resets is 10 minutes.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the trap generation to 10 minutes before the scheduled resets:

```
(Cisco Controller) > reset system notify-time 55
```

reset peer-system

To reset the peer controller, use the **reset peer-system** command.

reset peer-system

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to reset the peer controller:

```
(Cisco Controller) >> reset peer-system
```

save config

To save the controller configurations, use the **save config** command.

save config

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to save the controller settings:

```
(Cisco Controller) > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
```

transfer download certpasswor

To set the password for the .PEM file so that the operating system can decrypt the web administration SSL key and certificate, use the **transfer download certpassword** command.

transfer download certpassword *private_key_password*

Syntax Description

private_key_password	Certificate's private key password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file to the switch with the certificate's private key password certpassword:

```
(Cisco Controller) > transfer download certpassword
Clearing password
```

transfer download datatype

To set the download file type, use the **transfer download datatype** command.

transfer download datatype {**code** | **config** | **eapdevcert** | **eapcacert** | **icon** | **image** | **ipseccacert** | **ipsecdevcert** | **login-banner** | **radius-avplist** | **signature** | **webadmincert** | **webauthbundle** | **webauthcert**}

Syntax Description

code	Downloads an executable image to the system.
config	Downloads the configuration file.
eapcacert	Downloads an EAP ca certificate to the system.
eapdevcert	Downloads an EAP dev certificate to the system.
icon	Downloads an executable image to the system.
image	Downloads a web page login to the system.
ipseccacert	Downloads an IPSec Certificate Authority (CA) certificate to the system.
ipsecdevcert	Downloads an IPSec dev certificate to the system.
login-banner	Downloads the controller login banner. Only text file is supported with a maximum of 1500 bytes.
radius-avplist	Downloads the RADIUS AVPs in the XML file format from the FTP server.
signature	Downloads a signature file to the system.
webadmincert	Downloads a certificate for web administration to the system.
webauthbundle	Downloads a custom webauth bundle to the system.
webauthcert	Downloads a web certificate for the web portal to the system.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The **ipseccacert**, **ipsecdevcert**, and **radius-avplist** options were introduced.

The following example shows how to download an executable image to the system:

```
(Cisco Controller) > transfer download datatype code
```

transfer download datatype icon

To download icon from TFTP or FTP server onto the controller, use the **transfer download datatype icon** command.

transfer download datatype icon

Syntax Description

None

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Release 8.2	This command was introduced.

Usage Guidelines

Example

This example shows how to download icon from TFTP or FTP server onto the controller:

```
Cisco Controller > transfer download datatype icon
```

transfer download filename

To download a specific file, use the **transfer download filename** command.

transfer download filename *filename*

Syntax Description

filename	Filename that contains up to 512 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to transfer a file named build603:

```
(Cisco Controller) > transfer download filename build603
```

transfer download mode

To set the transfer mode, use the **transfer download mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description

ftp	Sets the transfer mode to FTP.
tftp	Sets the transfer mode to TFTP.
sftp	Sets the transfer mode to SFTP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file using the TFTP mode:

```
(Cisco Controller) > transfer download mode tftp
```

transfer download password

To set the password for an FTP transfer, use the **transfer download password** command.

transfer download password *password*

Syntax Description

password	Password.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the password for FTP transfer to pass01:

```
(Cisco Controller) > transfer download password pass01
```

transfer download path

To set a specific FTP or TFTP path, use the **transfer download path** command.

transfer download path *path*

Syntax Description

path	Directory path.

Note Path names on a TFTP or FTP server are relative to the server's default or root directory. For example, in the case of the Solarwinds TFTP server, the path is "/".

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to transfer a file to the path c:\install\version2:

```
(Cisco Controller) > transfer download path c:\install\version2
```

transfer download port

To specify the FTP port, use the **transfer download port** command.

transfer download port *port*

Syntax Description

port	FTP port.

Command Default

The default FTP *port* is 21.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify FTP port number 23:

```
(Cisco Controller) > transfer download port 23
```

transfer download serverip

To configure the IPv4 or IPv6 address of the TFTP server from which to download information, use the **transfer download serverip** command.

transfer download serverip *IP addr*

Syntax Description

IP addr	TFTP server IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to configure the IPv4 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 175.34.56.78
```

The following example shows how to configure the IPv6 address of the TFTP server:

```
(Cisco Controller) > transfer download serverip 2001:10:1:1::1
```

transfer download start

To initiate a download, use the **transfer download start** command.

transfer download start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate a download:

```
(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

To specify the TFTP packet timeout, use the **transfer download tftpPktTimeout** command.

transfer download tftpPktTimeout *timeout*

Syntax Description

timeout	Timeout in seconds between 1 and 254.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to transfer a file with the TFTP packet timeout of 55 seconds:

```
(Cisco Controller) > transfer download tftpPktTimeout 55
```

transfer download tftpMaxRetries

To specify the number of allowed TFTP packet retries, use the **transfer download tftpMaxRetries** command.

transfer download tftpMaxRetries *retries*

Syntax Description

retries	Number of allowed TFTP packet retries between 1 and 254 seconds.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the number of allowed TFTP packet retries to 55:

```
(Cisco Controller) > transfer download tftpMaxRetries 55
```

transfer download username

To specify the FTP username, use the **transfer download username** command.

transfer download username *username*

Syntax Description

username	Username.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer download username ftp_username
```

transfer encrypt

To configure encryption for configuration file transfers, use the **transfer encrypt** command.

transfer encrypt {**enable** | **disable** | **set-key** *key*}

Syntax Description

enable	Enables the encryption settings.
disable	Disables the encryption settings.
set-key	Specifies the encryption key for configuration file transfers.
key	Encryption key for config file transfers.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to enable the encryption settings:

```
(Cisco Controller) > transfer encrypt enable
```

transfer upload datatype

To set the controller to upload specified log and crash files, use the **transfer upload datatype** command.

transfer upload datatype { **ap-crash-data** | **config** | **coredump** | **crashfile** | **debug-file** | **eapcacert** | **eapdevcert** | **errorlog** | **invalid-config** | **pac** | **packet-capture** | **panic-crash-file** | **radio-core-dump** | **radius-avplist** | **rrm-log** | **run-config** | **signature** | **systemtrace** | **traplog** | **watchdog-crash-file webadmincert** | **webauthbundle** | **webauthcert** }

Syntax Description

ap-crash-data	Uploads the AP crash files.
config	Uploads the system configuration file.
coredump	Uploads the core-dump file.
crashfile	Uploads the system crash file.
debug-file	Uploads the system's debug log file.
eapcacert	Uploads an EAP CA certificate.
eapdevcert	Uploads an EAP Dev certificate.
errorlog	Uploads the system error log file.
invalid-config	Uploads the system invalid-config file.
pac	Uploads a Protected Access Credential (PAC).
packet-capture	Uploads a packet capture file.
panic-crash-file	Uploads the kernel panic information file.
radio-core-dump	Uploads the system error log.
radius-avplist	Uploads the XML file from the controller to the RADIUS server.
rrm-log	Uploads the system's trap log.
run-config	Upload the controller's running configuration
signature	Uploads the system signature file.
systemtrace	Uploads the system trace file.
traplog	Uploads the system trap log.
watchdog-crash-file	Uploads a console dump file resulting from a software-watchdog-initiated controller reboot following a crash.
webadmincert	Uploads Web Admin certificate.
webauthbundle	Uploads a Web Auth bundle.

webauthcert	Upload a web certificate

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	The **ipseccacert**, **ipsecdevcert**, and **radius-avplist** options were introduced.

The following example shows how to upload the system error log file:

```
(Cisco Controller) > transfer upload datatype errorlog
```

transfer upload filename

To upload a specific file, use the **transfer upload filename** command.

transfer upload filename *filename*

Syntax Description

filename	Filename that contains up to 16 alphanumeric characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the filename.

The following example shows how to upload a file build603:

```
(Cisco Controller) > transfer upload filename build603
```

transfer upload mode

To configure the transfer mode, use the **transfer upload mode** command.

transfer upload mode {**ftp** | **tftp** | **sftp**}

Syntax Description

ftp	Sets the transfer mode to FTP.
tftp	Sets the transfer mode to TFTP.
sftp	Sets the transfer mode to SFTP.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the transfer mode to TFTP:

```
(Cisco Controller) > transfer upload mode tftp
```

transfer upload pac

To load a Protected Access Credential (PAC) to support the local authentication feature and allow a client to import the PAC, use the **transfer upload pac** command.

transfer upload pac *username validity password*

Syntax Description

username	User identity of the PAC.
validity	Validity period (days) of the PAC.
password	Password to protect the PAC.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

The client upload process uses a TFTP or FTP server.

The following example shows how to upload a PAC with the username user1, validity period 53, and password pass01:

```
(Cisco Controller) > transfer upload pac user1 53 pass01
```

transfer upload password

To configure the password for FTP transfer, use the **transfer upload password** command.

Syntax Description

password	Password needed to access the FTP server.

transfer upload password *password*

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to configure the password for the FTP transfer to pass01:

```
(Cisco Controller) > transfer upload password pass01
```

transfer upload path

To set a specific upload path, use the **transfer upload path** command.

transfer upload path *path*

Syntax Description

path	Server path to file.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

Usage Guidelines

You cannot use special characters such as \ : * ? " < > | for the file path.

The following example shows how to set the upload path to c:\install\version2:

```
(Cisco Controller) > transfer upload path c:\install\version2
```

transfer upload peer-start

To upload a file to the peer controller, use the **transfer upload peer-start** command.

transfer upload peer-start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to start uploading a file to the peer controller:

```
(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

To specify the FTP port, use the **transfer upload port** command.

transfer upload port *port*

Syntax Description

port	Port number.

Command Default

The default FTP port is 21.

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to specify FTP port 23:

```
(Cisco Controller) > transfer upload port 23
```

transfer upload serverip

To configure the IPv4 or IPv6 address of the TFTP server to upload files to, use the **transfer upload serverip** command.

transfer upload serverip *IP addr*

Syntax Description

IP addr	TFTP Server IPv4 or IPv6 address.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.
8.0	This command supports both IPv4 and IPv6 address formats.

The following example shows how to set the IPv4 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 175.31.56.78
```

The following example shows how to set the IPv6 address of the TFTP server to 175.31.56.78:

```
(Cisco Controller) > transfer upload serverip 2001:10:1:1::1
```

transfer upload start

To initiate an upload, use the **transfer upload start** command.

transfer upload start

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to initiate an upload of a file:

```
(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

To specify the FTP username, use the **transfer upload username** command.

transfer upload username

Syntax Description

username	Username required to access the FTP server. The username can contain up to 31 characters.

Command Default

None

Command History

Release	Modification
7.6	This command was introduced in a release earlier than Release 7.6.

The following example shows how to set the FTP username to ftp_username:

```
(Cisco Controller) > transfer upload username ftp_username
```