Command Reference, Cisco IOS XE Denali 16.1.x (Catalyst 3850 Switches)

First Published: 2015-11-30

Last Modified: 2016-04-21

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

© 2016 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface

Preface xxxi

Document Conventions xxxi

Related Documentation xxxiii

Obtaining Documentation and Submitting a Service Request xxxiii

CHAPTER 1

Using the Command-Line Interface 1

Using the Command-Line Interface 1

Understanding Command Modes 1

Understanding the Help System 3

Understanding Abbreviated Commands 4

Understanding no and default Forms of Commands 4

Understanding CLI Error Messages 4

Using Configuration Logging 5

Using Command History 5

Changing the Command History Buffer Size 5

Recalling Commands 5

Disabling the Command History Feature 6

Using Editing Features 6

Enabling and Disabling Editing Features 6

Editing Commands through Keystrokes 7

Editing Command Lines that Wrap 9

Searching and Filtering Output of show and more Commands 9

Accessing the CLI 10

Accessing the CLI through a Console Connection or through Telnet 10

PART I

CleanAir 11

CHAPTER 2 CleanAir Commands 13

ap dot11 5ghz cleanair 14
ap dot11 5ghz cleanair alarm air-quality 14
ap dot11 5ghz cleanair alarm device 15
default ap dot11 5ghz cleanair device 16
ap dot11 5ghz rrm channel cleanair-event 17
ap dot11 5ghz rrm channel device 18
ap dot11 24ghz cleanair 19
ap dot11 24ghz cleanair alarm air-quality 19
ap dot11 24ghz cleanair alarm device 20
default ap dot11 24ghz cleanair device 21
ap dot11 24ghz rrm channel cleanair-event 23
ap dot11 24ghz rrm channel device 23
ap name mode se-connect 24
default ap dot11 5ghz cleanair device 25
default ap dot11 5ghz rrm channel cleanair-event 26
default ap dot11 5ghz rrm channel device 27
default ap dot11 24ghz cleanair alarm device 27
default ap dot11 24ghz cleanair device 29
default ap dot11 24ghz rrm channel cleanair-event 30
show ap dot11 5ghz cleanair air-quality summary 31
show ap dot11 5ghz cleanair air-quality worst 31
show ap dot11 5ghz cleanair config 32
show ap dot11 5ghz cleanair device type 34
show ap dot11 24ghz cleanair air-quality summary 35
show ap dot11 24ghz cleanair air-quality worst 36
show ap dot11 24ghz cleanair config 36
show ap dot11 24ghz cleanair summary 38

PART II Flexible NetFlow Commands 39

CHAPTER 3 Flexible NetFlow Commands 41

cache 42
clear flow exporter 44

clear flow monitor 45
collect 46
collect counter 47
collect interface 48
collect timestamp absolute 49
collect transport tcp flags 50
datalink flow monitor 51
debug flow exporter 52
debug flow monitor 53
debug flow record 53
debug sampler 54
description 55
destination 56
dscp 57
export-protocol netflow-v9 57
exporter 58
flow exporter 59
flow monitor 60
flow record 60
ip flow monitor 61
ipv6 flow monitor 62
match datalink ethertype 64
match datalink mac 65
match datalink vlan 66
match flow direction 66
match interface 67
match ipv4 68
match ipv4 destination address 69
match ipv4 source address 70
match ipv4 ttl 71
match ipv6 71
match ipv6 destination address 72
match ipv6 hop-limit 73
match ipv6 source address 74
match transport 74

match transport icmp ipv4 75
match transport icmp ipv6 76
mode random 1 out-of 77
option 78
record 79
sampler 80
show flow exporter 81
show flow interface 83
show flow monitor 84
show flow record 89
show sampler 89
source 91
template data timeout 93
transport 93
ttl 94

PART III Interface and Hardware Components 97

CHAPTER 4 Interface and Hardware Commands 99

client vlan 101
debug ilpower 102
debug interface 103
debug lldp packets 104
debug nmsp 105
debug platform poe 106
duplex 106
errdisable detect cause 108
errdisable recovery cause 110
errdisable recovery interval 112
interface 113
interface range 114
ip mtu 115
ipv6 mtu 116
lldp (interface configuration) 117
logging event power-inline-status 118

mdix auto 119
mode (power-stack configuration) 120
network-policy 121
network-policy profile (global configuration) 122
nmsp attachment suppress 123
power efficient-ethernet auto 124
power-priority 124
power inline 126
power inline police 129
power supply 131
show CAPWAP summary 132
show controllers cpu-interface 133
show controllers ethernet-controller 134
show controllers utilization 143
show eee 144
show env 147
show errdisable detect 150
show errdisable recovery 151
show interfaces 152
show interfaces counters 156
show interfaces switchport 158
show interfaces transceiver 160
show memory platform 162
show module 164
show mgmt-infra trace messages ilpower 165
show mgmt-infra trace messages ilpower-ha 166
show mgmt-infra trace messages platform-mgr-poe 166
show network-policy profile 167
show platform CAPWAP summary 168
show platform forward 169
show platform hardware fed switch forward 170
show platform resources 172
show platform software ilpower 173
show platform software process list 174
show platform software process slot switch 176

show platform software status control-processor 178
show processes cpu platform monitor 181
show processes memory platform 182
show power inline 185
show stack-power 190
show stack-power 192
show system mtu 192
show tech-support 193
show wireless interface summary 195
speed 195
stack-power 197
switchport block 198
system mtu 199
test mcu read-register 200
voice-signaling vlan (network-policy configuration) 202
voice vlan (network-policy configuration) 203
wireless ap-manager interface 204
wireless exclusionlist 205
wireless linktest 206
wireless management interface 207
wireless peer-blocking forward-upstream 207

PART IV IP Multicast Routing Commands 209

CHAPTER 5 IP Multicast Commands 211

cache-memory-max 212
clear ip mfib counters 213
clear ip mroute 214
ip igmp filter 215
ip igmp max-groups 216
ip igmp profile 218
ip igmp snooping 219
ip igmp snooping last-member-query-count 220
ip igmp snooping querier 221
ip igmp snooping report-suppression 223

ip igmp snooping vlan mrouter 224
ip igmp snooping vlan static 225
ip multicast auto-enable 226
ip multicast vlan 226
ip pim accept-register 227
ip pim bsr-candidate 228
ip pim rp-candidate 230
ip pim send-rp-announce 231
ip pim spt-threshold 232
match message-type 233
match service-type 234
match service-instance 234
mrinfo 235
redistribute mdns-sd 236
service-list mdns-sd 237
service-policy-query 238
service-routing mdns-sd 239
service-policy 240
show ip igmp filter 240
show ip igmp profile 241
show ip igmp snooping 242
show ip igmp snooping groups 244
show ip igmp snooping igmpv2-tracking 245
show ip igmp snooping mrouter 245
show ip igmp snooping querier 246
show ip igmp snooping wireless mcast-spi-count 248
show ip igmp snooping wireless mgid 248
show ip pim autorp 249
show ip pim bsr-router 250
show ip pim bsr 251
show ip pim tunnel 252
show mdns cache 253
show mdns requests 254
show mdns statistics 255
show platform ip multicast 256

wireless mdns-bridging 263
wireless multicast 263

PART V IPv6 265

CHAPTER 6 IPv6 Commands 267
ipv6 flow monitor 267
ipv6 traffic-filter 268
show wireless ipv6 statistics 269

PART VI Layer 2/3 271

CHAPTER 7 Layer 2/3 Commands 273
channel-group 274
channel-protocol 277
clear lacp 278
clear pagp 279
clear spanning-tree counters 279
clear spanning-tree detected-protocols 280
debug etherchannel 281
debug lacp 282
debug pagp 283
debug platform pm 284
debug platform udld 286
debug spanning-tree 286
interface port-channel 288
lacp max-bundle 289
lacp port-priority 290
lacp rate 291
lacp system-priority 292
pagp learn-method 293
pagp port-priority 294
port-channel 295
port-channel auto 295
port-channel load-balance 296

port-channel load-balance extended 297
port-channel min-links 299
rep admin vlan 300
rep block port 300
rep lsl-age-timer 302
rep lsl-retries 302
rep preempt delay 303
rep preempt segment 304
rep segment 305
rep stcn 306
show etherchannel 307
show interfaces rep detail 309
show lacp 310
show pagp 314
show platform etherchannel 315
show platform pm 316
show rep topology 317
show udld 318
switchport 322
switchport access vlan 323
switchport mode 324
switchport nonegotiate 326
switchport voice vlan 327
udld 329
udld port 330
udld reset 332

PART VII Lightweight Access Point 333

CHAPTER 8 Cisco Lightweight Access Point Commands 335

ap auth-list ap-policy 341
ap bridging 341
ap capwap multicast 342
ap capwap retransmit 343
ap capwap timers 344

ap cdp 345
ap core-dump 346
ap country 347
ap crash-file 348
ap dot11 24ghz preamble 349
ap dot11 24ghz dot11g 349
ap dot11 5ghz channelswitch mode 350
ap dot11 5ghz power-constraint 351
ap dot11 beaconperiod 352
ap dot11 beamforming 353
ap dot11 cac media-stream 354
ap dot11 cac multimedia 356
ap dot11 cac video 357
ap dot11 cac voice 358
ap dot11 cleanair 361
ap dot11 cleanair alarm air-quality 362
ap dot11 cleanair alarm device 363
ap dot11 cleanair device 364
ap dot11 dot11n 365
ap dot11 dtpc 368
ap dot11 edca-parameters 369
ap dot11 rrm group-mode 370
ap dot11 rrm channel cleanair-event 371
ap dot11 l2roam rf-params 372
ap dot11 media-stream 373
ap dot11 rrm ccx location-measurement 374
ap dot11 rrm channel dca 375
ap dot11 rrm group-member 377
ap dot11 rrm logging 378
ap dot11 rrm monitor 379
ap dot11 rrm ndp-type 380
ap dot11 5ghz dot11ac frame-burst 381
ap dot1x max-sessions 382
ap dot1x username 382
ap ethernet duplex 383

ap group 384
ap image 385
ap ipv6 tcp adjust-mss 386
ap led 387
ap link-encryption 387
ap link-latency 388
ap mgmtuser username 388
ap name ap-groupname 390
ap name antenna band mode 391
ap name bhrate 391
ap name bridgegroupname 392
ap name bridging 393
ap name cdp interface 393
ap name console-redirect 394
ap name capwap retransmit 395
ap name command 396
ap name core-dump 396
ap name country 397
ap name crash-file 398
ap name dot11 24ghz rrm coverage 399
ap name dot11 49ghz rrm profile 400
ap name dot11 5ghz rrm channel 402
ap name dot11 antenna 402
ap name dot11 antenna extantgain 404
ap name dot11 cleanair 404
ap name dot11 dot11n antenna 405
ap name dot11 dual-band cleanair 406
ap name dot11 dual-band shutdown 407
ap name dot11 rrm ccx 407
ap name dot11 rrm profile 408
ap name dot11 txpower 410
ap name dot1x-user 411
ap name ethernet 412
ap name ethernet duplex 413
ap name key-zeroize 414

ap name image 414
ap name ipv6 tcp adjust-mss 415
ap name jumbo mtu 416
ap name lan 416
ap name led 417
ap name link-encryption 418
ap name link-latency 418
ap name location 419
ap name mgmtuser 420
ap name mode 421
ap name monitor-mode 422
ap name monitor-mode dot11b 423
ap name name 424
ap name no dot11 shutdown 424
ap name power 425
ap name shutdown 426
ap name slot shutdown 426
ap name sniff 427
ap name ssh 428
ap name telnet 429
ap name power injector 429
ap name power pre-standard 430
ap name reset-button 431
ap name reset 431
ap name slot 432
ap name static-ip 433
ap name stats-timer 434
ap name syslog host 435
ap name syslog level 436
ap name tcp-adjust-mss 437
ap name tftp-downgrade 438
ap power injector 438
ap power pre-standard 439
ap reporting-period 440
ap reset-button 440

service-policy type control subscriber 441
ap static-ip 442
ap syslog 442
ap name no controller 444
ap tcp-adjust-mss size 445
ap tftp-downgrade 445
config wireless wps rogue client mse 446
clear ap name tsm dot11 all 447
clear ap config 448
clear ap eventlog-all 448
clear ap join statistics 449
clear ap mac-address 449
clear ap name wlan statistics 450
debug ap mac-address 451
show ap cac voice 451
show ap capwap 452
show ap cdp 454
show ap config dot11 454
show ap config dot11 dual-band summary 455
show ap config fnf 456
show ap config 456
show ap crash-file 457
show ap data-plane 457
show ap dot11 l2roam 458
show ap dot11 cleanair air-quality 459
show ap dot11 cleanair config 460
show ap dot11 cleanair summary 461
show ap dot11 461
show ap env summary 466
show ap ethernet statistics 467
show ap gps-location summary 467
show ap groups 468
show ap groups extended 468
show ap image 469
show ap is-supported 469

show ap join stats summary 470
show ap link-encryption 471
show ap mac-address 471
show ap monitor-mode summary 473
show ap name auto-rf 473
show ap name bhmode 475
show ap name bhrate 476
show ap name cac voice 476
show ap name config fnf 477
show ap name dot11 call-control 478
show ap name cable-modem 479
show ap name capwap retransmit 479
show ap name ccx rm 480
show ap name cdp 481
show ap name channel 481
show ap name config 482
show ap name config dot11 484
show ap name config slot 487
show ap name core-dump 490
show ap name data-plane 491
show ap name dot11 491
show ap name dot11 cleanair 494
show ap name env 495
show ap name ethernet statistics 495
show ap name eventlog 496
show ap gps-location summary 497
show ap name image 497
show ap name inventory 498
show ap name lan port 499
show ap name link-encryption 499
show ap name service-policy 500
show ap name tcp-adjust-mss 501
show ap name wlan 501
show ap name wlandot11 service policy 502
show ap slots 503

show ap summary 504
show ap tcp-adjust-mss 504
show ap universal summary 505
show ap uptime 505
show wireless ap summary 506
show wireless client ap 507
test ap name 508
test capwap ap name 508
trapflags ap 509

PART VIII Mobility 511

CHAPTER 9 Mobility Commands 513
mobility anchor 513
wireless mobility 515
wireless mobility controller 515
wireless mobility controller (ip_address) 517
wireless mobility controller peer-group 517
wireless mobility group keepalive 518
wireless mobility group member ip 519
wireless mobility group name 520
wireless mobility load-balance 521
show wireless mobility 522
clear wireless mobility statistics 523

PART IX Network Management 525

CHAPTER 10 Network Management Commands 527
ip wccp 528
monitor capture (interface/control plane) 530
monitor capture buffer 534
monitor capture clear 535
monitor capture export 535
monitor capture file 536
monitor capture limit 538

monitor capture match 539
monitor capture start 540
monitor capture stop 540
monitor session 541
monitor session destination 542
monitor session filter 546
monitor session source 547
show ip sla statistics 549
show monitor 550
show monitor capture 552
show platform ip wccp 553
show platform software swspan 554
snmp-server enable traps 556
snmp-server enable traps bridge 558
snmp-server enable traps bulkstat 559
snmp-server enable traps call-home 560
snmp-server enable traps cef 561
snmp-server enable traps cpu 562
snmp-server enable traps envmon 563
snmp-server enable traps errdisable 564
snmp-server enable traps flash 565
snmp-server enable traps isis 566
snmp-server enable traps license 566
snmp-server enable traps mac-notification 567
snmp-server enable traps ospf 568
snmp-server enable traps pim 569
snmp-server enable traps port-security 570
snmp-server enable traps power-ethernet 571
snmp-server enable traps snmp 572
snmp-server enable traps stackwise 573
snmp-server enable traps storm-control 575
snmp-server enable traps stpx 576
snmp-server enable traps transceiver 577
snmp-server enable traps vrfmib 578
snmp-server enable traps vstack 579

snmp-server engineID 580
snmp-server host 580
switchport mode access 585
switchport voice vlan 586

PART X QoS 587

CHAPTER 11 QoS Commands 589
class 590
class-map 592
match (class-map configuration) 593
match non-client-nrt 596
match wlan user-priority 597
policy-map 597
priority 599
queue-buffers ratio 601
queue-limit 603
service-policy (Wired) 604
service-policy (WLAN) 605
set 606
show ap name service-policy 612
show ap name dot11 613
show class-map 615
show platform hardware fed switch 616
show platform software fed switch qos 619
show platform software fed switch qos qsb 620
show wireless client calls 622
show wireless client dot11 623
show wireless client mac-address (Call Control) 624
show wireless client mac-address (TCLAS) 625
show wireless client voice diagnostics 625
show policy-map 626
show wlan 628
trust device 630

PART XI Radio Resource Management 633

CHAPTER 12 Radio Resource Management Commands 635

ap dot11 rrm 635
ap dot11 rrm ccx 638
ap dot11 rrm channel 638
ap dot11 24ghz rrm channel cleanair-event rogue-contribution 639
ap dot11 24ghz or 5ghz rrm channel dca add 640
ap dot11 24ghz or 5ghz rrm channel dca remove 641
ap dot11 5ghz rrm channel dca chan-width-11n 642
ap dot11 rrm coverage 642
ap dot11 rrm group-member 644
ap dot11 rrm monitor 644
ap dot11 rrm profile 645
ap dot11 rrm tpc-threshold 646
ap dot11 rrm txpower 647
show ap dot11 24ghz 648
show ap dot11 5ghz 649

PART XII Security 651

CHAPTER 13 Security Commands 653

aaa accounting 655
aaa accounting dot1x 658
aaa accounting identity 659
aaa authentication dot1x 661
aaa authorization 662
aaa new-model 666
access-session mac-move deny 667
action 669
authentication host-mode 670
authentication mac-move permit 671
authentication priority 672
authentication violation 675

clear errdisable interface vlan 676
clear mac address-table 677
deny (MAC access-list configuration) 678
device-role (IPv6 snooping) 682
device-role (IPv6 nd inspection) 682
device-tracking policy 683
dot1x critical (global configuration) 685
dot1x max-start 685
dot1x test eapol-capable 686
dot1x test timeout 687
dot1x timeout 688
epm access-control open 690
ip admission 691
ip admission name 692
ip device tracking maximum 694
ip device tracking probe 695
ip dhcp snooping database 696
ip dhcp snooping information option format remote-id 697
ip dhcp snooping verify no-relay-agent-address 698
ip http access-class 699
ip source binding 700
ip verify source 701
ipv6 access-list 702
ipv6 snooping policy 704
limit address-count 705
mab request format attribute 32 706
match (access-map configuration) 707
no authentication logging verbose 709
no dot1x logging verbose 709
no mab logging verbose 710
permit (MAC access-list configuration) 711
protocol (IPv6 snooping) 714
security level (IPv6 snooping) 715
security passthru 716
show aaa clients 717

show aaa command handler 717
show aaa local 718
show aaa servers 719
show aaa sessions 720
show authentication history 721
show authentication sessions 721
show dot1x 724
show eap pac peer 725
show ip dhcp snooping statistics 725
show radius server-group 728
show storm-control 729
show vlan access-map 731
show vlan filter 732
show vlan group 732
storm-control 733
switchport port-security aging 736
switchport port-security mac-address 737
switchport port-security maximum 739
switchport port-security violation 741
tracking (IPv6 snooping) 742
trusted-port 744
wireless dot11-padding 745
wireless security dot1x 745
wireless security lsc 747
wireless security strong-password 748
wireless wps ap-authentication 749
wireless wps auto-immune 750
wireless wps cids-sensor 750
wireless wps client-exclusion 751
wireless wps mfp infrastructure 752
wireless wps rogue 753
wireless wps shun-list re-sync 754
vlan access-map 754
vlan filter 756
vlan group 757

PART XIII Stack Manager and High Availability 759

CHAPTER 14 Stack Manager and High Availability Commands 761

debug platform stack-manager 762
main-cpu 763
mode sso 763
policy config-sync prc reload 764
redundancy 765
redundancy config-sync mismatched-commands 766
redundancy force-switchover 767
redundancy reload 768
reload 769
session 770
set trace capwap ap ha 771
set trace mobility ha 772
set trace qos ap ha 774
show checkpoint 775
show etherchannel summary 780
show platform ses 781
show platform stack-manager 786
show redundancy 787
show redundancy config-sync 790
show switch 792
show trace messages capwap ap ha 796
show trace messages mobility ha 797
stack-mac persistent timer 798
stack-mac update force 799
standby console enable 800
switch stack port 801
switch priority 802
switch provision 802
switch renumber 804

PART XIV System Management 807

CHAPTER 15 System Management Commands 809

arp 812

boot 812

cat 813

clear location 814

clear location statistics 815

clear nmsp statistics 816

clear wireless ccx statistics 816

clear wireless client tsm dot11 817

clear wireless location s69 statistics 818

copy 818

copy startup-config tftp: 819

copy tftp: startup-config 820

debug call-admission wireless all 821

debug rfid 821

debug voice diagnostics mac-address 822

debug wps mfp 823

delete 824

dir 825

emergency-install 826

exit 828

flash_init 828

help 829

license right-to-use 830

location 831

location algorithm 835

location expiry 835

location notify-threshold 836

location plm calibrating 837

location rfid 838

location rssi-half-life 839

mac address-table move update 840

mgmt_init 841

mkdir 842

more 842
nmsp notification interval 843
no debug all 844
rename 845
reset 846
rmdir 847
sdm prefer 847
set 848
show avc client 851
show avc wlan 851
show cable-diagnostics tdr 852
show debug 855
show env 856
show env xps 857
show flow monitor 861
show license right-to-use 865
show location 867
show location ap-detect 868
show mac address-table move update 869
show nmsp 870
show sdm prefer 871
show tech-support wireless 872
show wireless band-select 874
show wireless client calls 875
show wireless client dot11 876
show wireless client location-calibration 876
show wireless client probing 877
show wireless client summary 878
show wireless client timers 878
show wireless client voice diagnostics 879
show wireless country 880
show wireless detail 883
show wireless dtls connections 883
show wireless flow-control 884
show wireless flow-control statistics 885

show wireless load-balancing 886
show wireless performance 886
show wireless pmk-cache 887
show wireless probe 888
show wireless sip preferred-call-no 888
show wireless summary 889
shutdown 890
system env temperature threshold yellow 891
test cable-diagnostics tdr 892
traceroute mac 893
traceroute mac ip 895
trapflags 897
trapflags client 898
type 899
unset 900
version 901
wireless client 902
wireless client mac-address deauthenticate 903
wireless client mac-address 904
wireless load-balancing 909
wireless sip preferred-call-no 910

CHAPTER 16 **Tracing Commands** 911

Information About Tracing 911
Tracing Overview 911
Location of Tracelogs 912
Tracelog Naming Convention 912
Rotation and Throttling Policy 912
Tracing Levels 913
set platform software trace 913
show platform software trace filter-binary 917
show platform software trace message 918
show platform software trace level 921
request platform software trace archive 924
request platform software trace rotate all 925

request platform software trace filter-binary 925

PART XV VideoStream 927

CHAPTER 17 VideoStream Commands 929

ap dot11 media-stream multicast-direct 929

show ap dot11 930

show wireless media-stream group 931

wireless media-stream multicast-direct 932

wireless media-stream 933

PART XVI VLAN 935

CHAPTER 18 VLAN Commands 937

client vlan 938

clear vtp counters 939

debug platform vlan 939

debug sw-vlan 940

debug sw-vlan ifs 941

debug sw-vlan notification 942

debug sw-vlan vtp 943

interface vlan 945

show platform vlan 946

show vlan 946

show vtp 949

show wireless vlan group 955

switchport priority extend 956

switchport trunk 957

vlan 959

vlan dot1q tag native 965

vtp (global configuration) 965

vtp (interface configuration) 970

vtp primary 971

wireless broadcast vlan 972

PART XVII WLAN 973

CHAPTER 19 WLAN Commands 975

aaa-override 976
accounting-list 977
assisted-roaming 978
band-select 979
broadcast-ssid 980
call-snoop 981
channel-scan defer-priority 982
channel-scan defer-time 983
chd 984
client association limit 985
client vlan 986
ccx aironet-iesupport 987
datalink flow monitor 988
device-classification 989
default 990
dtim dot11 992
exclusionlist 993
exit 994
exit (WLAN AP Group) 994
ip access-group 995
ip flow monitor 996
ip verify source mac-check 997
load-balance 998
mobility anchor 999
nac 1000
passive-client 1001
peer-blocking 1002
radio 1003
radio-policy 1004
roamed-voice-client re-anchor 1005
security ft 1006

security pmf 1007
security web-auth 1008
security wpa akm 1009
service-policy (WLAN) 1010
session-timeout 1011
show wlan 1012
show wireless wlan summary 1014
shutdown 1015
sip-cac 1016
static-ip tunneling 1017
vlan 1018
universal-admin 1018
wgb non-cisco 1019
wifidirect policy 1020
wlan (AP Group Configuration) 1021
wlan 1022
wlan shutdown 1023
wmm 1023

Preface

- Document Conventions, page xxxi
- Related Documentation, page xxxiii
- Obtaining Documentation and Submitting a Service Request, page xxxiii

Document Conventions

This document uses the following conventions:

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

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

Reader Alert Conventions

This document may use the following conventions for reader alerts:

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

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

- Cisco Catalyst 3850 Switch documentation, located at:

  http://www.cisco.com/go/cat3850_docs

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

  http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html

- Cisco Validated Designs documents, located at:

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

- Error Message Decoder, located at:

  https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Obtaining Documentation and Submitting a Service Request

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

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

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

CHAPTER 1

Using the Command-Line Interface

This chapter contains the following topics:

- Using the Command-Line Interface, page 1

Using the Command-Line Interface

This chapter describes the Cisco IOS command-line interface (CLI) and how to use it to configure your switch.

Understanding Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

When you start a session on the switch, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode. The examples in the table use the hostname *Switch*.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session with your switch.	`Switch>`	Enter **logout** or **quit**.	Use this mode to • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the **enable** command.	`Device#`	Enter **disable** to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the **configure** command.	`Device(config)#`	To exit to privileged EXEC mode, enter **exit** or **end**, or press **Ctrl-Z**.	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the **vlan** *vlan-id* command.	`Device(config-vlan)#`	To exit to global configuration mode, enter the **exit** command. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the **interface** command (with a specific interface).	`Device(config-if)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
Line configuration	While in global configuration mode, specify a line with the **line vty** or **line console** command.	`Device(config-line)#`	To exit to global configuration mode, enter **exit**. To return to privileged EXEC mode, press **Ctrl-Z** or enter **end**.	Use this mode to configure parameters for the terminal line.

For more detailed information on the command modes, see the command reference guide for this release.

Understanding the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

Table 2: Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.

abbreviated-command-entry **?**
 	
`Device# di?`
`dir disable disconnect`
	Obtains a list of commands that begin with a particular character string.

abbreviated-command-entry <Tab>
 	
`Device# sh conf<tab>`
`Device# show configuration`
	Completes a partial command name.

? `Switch> ?`	Lists all commands available for a particular command mode.
command **?** `Switch> show ?`	Lists the associated keywords for a command.

command keyword **?**
 	
`Device(config)# cdp holdtime ?`
`  <10-255> Length of time (in sec) that receiver must keep this packet`
	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Device# show conf
```

Understanding no and default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

Understanding CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

Table 3: Common CLI Error Messages

Error Message	Meaning	How to Get Help
`% Ambiguous command: "show con"`	You did not enter enough characters for your switch to recognize the command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Incomplete command.`	You did not enter all the keywords or values required by this command.	Re-enter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
`% Invalid input detected at '^' marker.`	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Using Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.

Note Only CLI or HTTP changes are logged.

Using Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. These procedures are optional.

Beginning in privileged EXEC mode, enter this command to change the number of command lines that the switch records during the current terminal session:

```
Device# terminal history [size number-of-lines]
```

The range is from 0 to 256.

Beginning in line configuration mode, enter this command to configure the number of command lines the switch records for all sessions on a particular line:

```
Device(config-line)# history [size number-of-lines]
```

The range is from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 4: Recalling Commands

Action	Result
Press **Ctrl-P** or the up arrow key.	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Press **Ctrl-N** or the down arrow key.	Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the up arrow key. Repeat the key sequence to recall successively more recent commands.
show history `Device(config)# help`	While in privileged EXEC mode, lists the last several commands that you just entered. The number of commands that appear is controlled by the setting of the **terminal history** global configuration command and the **history** line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. These procedures are optional.

To disable the feature during the current terminal session, enter the **terminal no history** privileged EXEC command.

To disable command history for the line, enter the **no history** line configuration command.

Using Editing Features

This section describes the editing features that can help you manipulate the command line.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it, re-enable it, or configure a specific line to have enhanced editing. These procedures are optional.

To globally disable enhanced editing mode, enter this command in line configuration mode:

```
Switch (config-line)# no editing
```

To re-enable the enhanced editing mode for the current terminal session, enter this command in privileged EXEC mode:

```
Device# terminal editing
```

To reconfigure a specific line to have enhanced editing mode, enter this command in line configuration mode:

```
Device(config-line)# editing
```

Editing Commands through Keystrokes

This table shows the keystrokes that you need to edit command lines. These keystrokes are optional.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 5: Editing Commands through Keystrokes

Capability	Keystroke	Purpose
Move around the command line to make changes or corrections.	Press **Ctrl-B**, or press the left arrow key.	Moves the cursor back one character.
	Press **Ctrl-F**, or press the right arrow key.	Moves the cursor forward one character.
	Press **Ctrl-A**.	Moves the cursor to the beginning of the command line.
	Press **Ctrl-E**.	Moves the cursor to the end of the command line.
	Press **Esc B**.	Moves the cursor back one word.
	Press **Esc F**.	Moves the cursor forward one word.
	Press **Ctrl-T**.	Transposes the character to the left of the cursor with the character located at the cursor.
Recall commands from the buffer and paste them in the command line. The switch provides a buffer with the last ten items that you deleted.	Press **Ctrl-Y.**	Recalls the most recent entry in the buffer.
	Press **Esc Y**.	Recalls the next buffer entry. The buffer contains only the last 10 items that you have deleted or cut. If you press **Esc Y** more than ten times, you cycle to the first buffer entry.
Delete entries if you make a mistake or change your mind.	Press the **Delete** or **Backspace** key.	Erases the character to the left of the cursor.

Capability	Keystroke	Purpose
	Press **Ctrl-D**.	Deletes the character at the cursor.
	Press **Ctrl-K**.	Deletes all characters from the cursor to the end of the command line.
	Press **Ctrl-U** or **Ctrl-X**.	Deletes all characters from the cursor to the beginning of the command line.
	Press **Ctrl-W**.	Deletes the word to the left of the cursor.
	Press **Esc D**.	Deletes from the cursor to the end of the word.
Capitalize or lowercase words or capitalize a set of letters.	Press **Esc C**.	Capitalizes at the cursor.
	Press **Esc L**.	Changes the word at the cursor to lowercase.
	Press **Esc U**.	Capitalizes letters from the cursor to the end of the word.
Designate a particular keystroke as an executable command, perhaps as a shortcut.	Press **Ctrl-V** or **Esc Q**.	
Scroll down a line or screen on displays that are longer than the terminal screen can display. **Note** The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including **show** command output. You can use the **Return** and **Space** bar keystrokes whenever you see the More prompt.	Press the **Return** key.	Scrolls down one line.
	Press the **Space** bar.	Scrolls down one screen.
Redisplay the current command line if the switch suddenly sends a message to your screen.	Press **Ctrl-L** or **Ctrl-R**.	Redisplays the current command line.

Editing Command Lines that Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

In this example, the **access-list** global configuration command entry extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign ($) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Device(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Device(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Device(config)# $108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

After you complete the entry, press **Ctrl-A** to check the complete syntax before pressing the **Return** key to execute the command. The dollar sign ($) appears at the end of the line to show that the line has been scrolled to the right:

```
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1$
```

The software assumes that you have a terminal screen that is 80 columns wide. If you have a width other than that, use the **terminal width** privileged EXEC command to set the width of your terminal.

Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

To use this functionality, enter a **show** or **more** command followed by the pipe character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search for or filter out:

command | {**begin** | **include** | **exclude**} *regular-expression*

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

This example shows how to include in the output display only lines where the expression *protocol* appears:

```
Device# show interfaces | include protocol
Vlan1 is up, line protocol is up
Vlan10 is up, line protocol is down
GigabitEthernet1/0/1 is up, line protocol is down
GigabitEthernet1/0/2 is up, line protocol is up
```

Accessing the CLI

You can access the CLI through a console connection, through Telnet, or by using the browser.

You manage the switch stack and the stack member interfaces through the active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions to the active switch. Commands you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.

Note We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

To debug a specific stack member, you can access it from the active switch by using the **session** *stack-member-number* privileged EXEC command. The stack member number is appended to the system prompt. For example, *Switch-2#* is the prompt in privileged EXEC mode for stack member 2, and where the system prompt for the active switch is Switch. Only the **show** and **debug** commands are available in a CLI session to a specific stack member.

Accessing the CLI through a Console Connection or through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

CLI access is available before switch setup. After your switch is configured, you can access the CLI through a remote Telnet session or SSH client.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.
- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.

  The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.

  The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.

PART I

CleanAir

- CleanAir Commands, page 13

CHAPTER 2

CleanAir Commands

- ap dot11 5ghz cleanair , page 14
- ap dot11 5ghz cleanair alarm air-quality, page 14
- ap dot11 5ghz cleanair alarm device, page 15
- default ap dot11 5ghz cleanair device, page 16
- ap dot11 5ghz rrm channel cleanair-event, page 17
- ap dot11 5ghz rrm channel device, page 18
- ap dot11 24ghz cleanair, page 19
- ap dot11 24ghz cleanair alarm air-quality, page 19
- ap dot11 24ghz cleanair alarm device, page 20
- default ap dot11 24ghz cleanair device, page 21
- ap dot11 24ghz rrm channel cleanair-event, page 23
- ap dot11 24ghz rrm channel device, page 23
- ap name mode se-connect, page 24
- default ap dot11 5ghz cleanair device, page 25
- default ap dot11 5ghz rrm channel cleanair-event, page 26
- default ap dot11 5ghz rrm channel device, page 27
- default ap dot11 24ghz cleanair alarm device, page 27
- default ap dot11 24ghz cleanair device, page 29
- default ap dot11 24ghz rrm channel cleanair-event, page 30
- show ap dot11 5ghz cleanair air-quality summary, page 31
- show ap dot11 5ghz cleanair air-quality worst, page 31
- show ap dot11 5ghz cleanair config, page 32
- show ap dot11 5ghz cleanair device type, page 34
- show ap dot11 24ghz cleanair air-quality summary, page 35

- show ap dot11 24ghz cleanair air-quality worst, page 36
- show ap dot11 24ghz cleanair config, page 36
- show ap dot11 24ghz cleanair summary, page 38

ap dot11 5ghz cleanair

To enable CleanAir for detecting 5-GHz devices, use the **ap dot11 5ghz cleanair** command in global configuration mode.

ap dot11 5ghz cleanair

Command Default

Disabled.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 5-GHz devices:

```
Device(config)# ap dot11 5ghz cleanair
```

ap dot11 5ghz cleanair alarm air-quality

To configure the alarm when the Air Quality (AQ) reaches the threshold value for the 5-GHz devices, use the **ap dot11 5ghz cleanair alarm air-quality** command. To disable the alarm when the AQ reaches the threshold value for the 5-GHz devices, use the **no** form of this command.

ap dot11 5ghz cleanair alarm air-quality threshold *threshold _value*

Syntax Description

threshold *threshold _value*	Configures the threshold value for air quality. The range is from 1 to 100.

Command Default

The default threshold value for AQ is 10.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair**command before you configure this command.

This example shows how to set the threshold value for the AQ:

```
Device(config)# ap dot11 5ghz cleanair alarm air-quality threshold 30
```

ap dot11 5ghz cleanair alarm device

To configure the alarm for the 5-GHz interference devices, use the **ap dot11 5ghz cleanair alarm device** command.

ap dot11 5ghz cleanair alarm device {**canopy** | **cont-tx** | **dect-like** | **inv** | **jammer** | **nonstd** | **radar** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile**}

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
radar	Configures the alarm for radars.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled and for all other interference devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable the alarm to notify interferences from a radar device:

```
Device(config)# ap dot11 5ghz cleanair alarm device radar
```

default ap dot11 5ghz cleanair device

To configure the default state of the alarm for 5-GHz interference devices, use the **default ap dot11 5ghz cleanair device** command in global configuration mode.

default ap dot11 5ghz cleanair device {**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
radar	Configures the alarm for radars.
report	Enables interference device reports.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.

video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other interference devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 5ghz cleanair device video
```

ap dot11 5ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and configure the sensitivity for 5-GHz devices, use the **ap dot11 5ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of the command.

ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

no ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high**| **low**| **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the EDRRM sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 5ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to high:

```
Device(config)# ap dot11 5ghz rrm channel cleanair-event
Device(config)# ap dot11 5ghz rrm channel cleanair-event sensitivity high
```

ap dot11 5ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11a channel, use the **ap dot11 5ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 5ghz rrm channel device

no ap dot11 5ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

The CleanAir persistent device state is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance on 802.11a devices:

```
Device(config)# ap dot11 5ghz rrm channel device
```

ap dot11 24ghz cleanair

To enable CleanAir for detecting 2.4-GHz devices, use the **ap dot11 24ghz cleanair** command in global configuration mode. To disable CleanAir for detecting 2.4-GHz devices, use the **no** form of this command.

ap dot11 24ghz cleanair

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable this CleanAir command before you configure other CleanAir commands.

This example shows how to enable CleanAir for 2.4-GHz devices:

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 24ghz cleanair alarm air-quality

To configure the alarm for the threshold value of Air Quality (AQ) for all 2.4-GHz devices, use the **ap dot11 24ghz cleanair alarm air-quality** command in global configuration mode. To disable the alarm for the threshold value of AQ for all 2.4-GHz devices, use the **no** form of this command.

ap dot11 24ghz cleanair alarm air-quality threshold *threshold_value*

Syntax Description

threshold *threshold_value*	Configures the threshold value for AQ. The range is from 1 to 100.

Command Default

The default threshold value for AQ is 10.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair** command before you configure this command.

This example shows how to set the threshold value for the AQ:

```
Device(config)# ap dot11 24ghz cleanair alarm air-quality threshold 50
```

ap dot11 24ghz cleanair alarm device

To configure the alarm for the 2.4-GHz interference devices, use the **ap dot11 24ghz cleanair alarm device** command in global configuration mode. To disable the alarm for the 2.4-GHz interference devices, use the **no** form of this command.

ap dot11 24ghz cleanairalarm {**device** | **bt-discovery** | **bt-link canopy**| **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven** | **nonstd** | **superag** | **tdd-tx video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**}

Syntax Description

bt-discovery	Configures the alarm for Bluetooth interference devices.
bt-link	Configures the alarm for any Bluetooth link.
canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
fh	Configures the alarm for 802.11 frequency hopping (FH) devices.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
mw-oven	Configures the alarm for microwave ovens.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.

tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
xbox	Configures the alarm for Xbox interference devices.
zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair** command before you configure this command.

This example shows how to enable the alarm to notify interferences from a Zigbee device:

```
Device(config)# ap dot11 24ghz cleanair alarm device zigbee
```

default ap dot11 24ghz cleanair device

To configure the default state of report generation for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair device** command in global configuration mode.

default ap dot11 24ghz cleanair device {**bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee**}

Syntax Description

bt-discovery	Configures the alarm for Bluetooth interference devices.
bt-link	Configures the alarm for any Bluetooth link.
canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.

dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
fh	Configures the alarm for 802.11 frequency hopping devices.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
mw-oven	Configures the alarm for microwave ovens.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
xbox	Configures the alarm for Xbox interference devices.
zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair**command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 24ghz cleanair device video
```

ap dot11 24ghz rrm channel cleanair-event

To enable Event-Driven RRM (EDRRM) and the sensitivity for 2.4-GHz devices, use the **ap dot11 24ghz rrm channel cleanair-event** command in global configuration mode. To disable EDRRM, use the **no** form of this command.

ap dot11 24ghz rrm channel cleanair-event sensitivity {**high | low | medium**}

no ap dot11 24ghz rrm channel cleanair-event [**sensitivity**{**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the air quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable EDRRM using the **ap dot11 24ghz rrm channel cleanair-event** command before you configure the sensitivity.

This example shows how to enable EDRRM and set the EDRRM sensitivity to low:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity low
```

ap dot11 24ghz rrm channel device

To configure persistent non-Wi-Fi device avoidance in the 802.11b channel, use the **ap dot11 24ghz rrm channel device** command in global configuration mode. To disable persistent device avoidance, use the **no** form of this command.

ap dot11 24ghz rrm channel device

no ap dot11 24ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent device avoidance is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CleanAir-capable monitor mode access points collect information about persistent devices on all configured channels and stores the information in the device. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance:

```
Device(config)# ap dot11 24ghz rrm channel device
```

ap name mode se-connect

To configure the access point for SE-Connect mode, use the **ap name** *ap_name* **mode se-connect** command in privileged exec mode.

ap name *ap_name* **mode se-connect**

Syntax Description

ap_name	Name of the access point.

Command Default

No access point is configured for SE-Connect mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The access point will reboot after you change the mode.

SE-connect mode enables a user to connect a Spectrum Expert application running on an external Microsoft Windows XP or Vista PC to a Cisco CleanAir-enabled access point in order to display and analyze detailed spectrum data. The Spectrum Expert application connects directly to the access point, by passing the controller. An access point in SE-Connect mode does not provide any Wi-Fi, RF, or spectrum data to the controller. All CleanAir system functionality is suspended while the AP is in this mode, and no clients are served. This mode is intended for remote troubleshooting only.

This example shows how to change the mode of the access point to SE-Connect:

```
Device# ap name AS-5508-5-AP3 mode se-connect

Changing the AP's mode will cause the AP to reboot.
Are you sure you want to continue? (y/n)[y]: y
% switch-1:wcm:Cisco AP does not support the seconnect mode
```

default ap dot11 5ghz cleanair device

To configure the default state of the alarm for 5-GHz interference devices, use the **default ap dot11 5ghz cleanair device** command in global configuration mode.

default ap dot11 5ghz cleanair device {**canopy | cont-tx | dect-like | inv | jammer | nonstd | radar | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}

Syntax Description

canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
radar	Configures the alarm for radars.
report	Enables interference device reports.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.

wimax-mobile	Configures the alarm for WiMax mobile interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other interference devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 5ghz cleanair** command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 5ghz cleanair device video
```

default ap dot11 5ghz rrm channel cleanair-event

To configure the default state of Event-Driven radio resource management (EDRRM) and the EDRRM sensitivity for 5-GHz devices, use the **default ap dot11 5ghz rrm channel cleanair-event** command in global configuration mode.

default ap dot11 5ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]

Syntax Description

sensitivity	(Optional) Configures the EDRRM sensitivity of the CleanAir event.
high	(Optional) Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the Air Quality (AQ) value.
low	(Optional) Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	(Optional) Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the sensitivity is low.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable EDRRM before you configure the sensitivity.

This example shows how to set the default EDRRM state and sensitivity:

```
Device(config)# default ap dot11 5ghz rrm channel cleanair-event
Device(config)# default ap dot11 5ghz rrm channel cleanair-event sensitivity
```

default ap dot11 5ghz rrm channel device

To configure the default state of the persistent non-Wi-Fi device avoidance in the 802.11a channels, use the **default ap dot11 5ghz rrm channel device** command in global configuration mode.

default ap dot11 5ghz rrm channel device

Syntax Description

This command has no arguments or keywords.

Command Default

Persistent device state is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This example shows how to configure persistent non-Wi-Fi device avoidance in the 802.11a channels:

```
Device(config)# default ap dot11 5ghz rrm channel device
```

default ap dot11 24ghz cleanair alarm device

To configure the default value of the alarm for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair alarm device** command in global configuration mode.

default ap dot11 24ghz cleanair alarm device {**bt-discovery** | **bt-link** | **canopy** | **cont-tx** | **dect-like** | **fh** | **inv** | **jammer** | **mw-oven**| **nonstd** | **superag** | **tdd-tx** | **video** | **wimax-fixed** | **wimax-mobile** | **xbox** | **zigbee**}

Syntax Description

bt-discovery	Configures the alarm for Bluetooth interference devices.
bt-link	Configures the alarm for any Bluetooth link.
canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
fh	Configures the alarm for 802.11 frequency hopping (FH) devices.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
mw-oven	Configures the alarm for microwave ovens.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
xbox	Configures the alarm for Xbox interference devices.
zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all the other devices is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair** command before you configure this command.

This example shows how to configure the default CleanAir 2.4-GHz interference devices alarm:

```
Device(config)# default ap dot11 24ghz cleanair alarm device inv
```

default ap dot11 24ghz cleanair device

To configure the default state of report generation for 2.4-GHz interference devices, use the **default ap dot11 24ghz cleanair device** command in global configuration mode.

default ap dot11 24ghz cleanair device {**bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee**}

Syntax Description

bt-discovery	Configures the alarm for Bluetooth interference devices.
bt-link	Configures the alarm for any Bluetooth link.
canopy	Configures the alarm for canopy interference devices.
cont-tx	Configures the alarm for continuous transmitters.
dect-like	Configures the alarm for Digital Enhanced Cordless Communication (DECT)-like phones.
fh	Configures the alarm for 802.11 frequency hopping devices.
inv	Configures the alarm for devices using spectrally inverted Wi-Fi signals.
jammer	Configures the alarm for jammer interference devices.
mw-oven	Configures the alarm for microwave ovens.
nonstd	Configures the alarm for devices using nonstandard Wi-Fi channels.
superag	Configures the alarm for 802.11 SuperAG interference devices.
tdd-tx	Configures the alarm for Time Division Duplex (TDD) transmitters.
video	Configures the alarm for video cameras.
wimax-fixed	Configures the alarm for WiMax fixed interference devices.
wimax-mobile	Configures the alarm for WiMax mobile interference devices.
xbox	Configures the alarm for Xbox interference devices.

zigbee	Configures the alarm for 802.15.4 interference devices.

Command Default

The alarm for Wi-Fi inverted devices is enabled. The alarm for all other devices is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable CleanAir using the **ap dot11 24ghz cleanair**command before you configure this command.

This example shows how to enable CleanAir to report when a video camera interferes:

```
Device(config)# default ap dot11 24ghz cleanair device video
```

default ap dot11 24ghz rrm channel cleanair-event

To configure the default Event-Driven radio resource management (EDRRM) state and sensitivity for 2.4-GHz devices, use the **default ap dot11 24ghz rrm channel cleanair-event** command in global configuration mode.

default ap dot11 24ghz rrm channel cleanair-event [**sensitivity** {**high** | **low** | **medium**}]

Syntax Description

sensitivity	Configures the EDRRM sensitivity of the CleanAir event.
high	Specifies the highest sensitivity to non-Wi–Fi interference as indicated by the Air Quality (AQ) value.
low	Specifies the least sensitivity to non-Wi–Fi interference as indicated by the AQ value.
medium	Specifies medium sensitivity to non-Wi–Fi interference as indicated by the AQ value.

Command Default

EDRRM is disabled and the sensitivity is low.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable EDRRM and set the default EDRRM sensitivity:

```
Device(config)# default ap dot11 24ghz rrm channel cleanair-event
Device(config)# default ap dot11 24ghz rrm channel cleanair-event sensitivity
```

show ap dot11 5ghz cleanair air-quality summary

To display the CleanAir AQ data for 5-GHz band, use the **show ap dot11 5ghz cleanair air-quality summary** command in user EXEC mode or privileged EXEC mode.

show ap dot11 5ghz cleanair air-quality summary

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the CleanAir AQ data for 5-GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP270ca.9b86.4546   1         99      99      0            No
AP2894.0f26.22df    6         98      97      0            No
AP2894.0f58.cc6b    11        99      99      0            No
AP2894.0f39.1040    6         97      97      0            No
AP2894.0f63.c6da    11        99      99      0            No
AP2894.0f58.d013    6         97      97      0            No
```

show ap dot11 5ghz cleanair air-quality worst

To display the worst AQ data for 5-GHz band, use the **show ap dot11 5ghz cleanair air-quality worst** command in user EXEC mode or privileged EXEC mode.

show ap dot11 5ghz cleanair air-quality worst

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the worst AQ data for 5-GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-------------------------------------------------------------
AP2894.0f39.1040    6         97      97      0            No
```

show ap dot11 5ghz cleanair config

To display the CleanAir configuration for 5-GHz band, use the **show ap dot11 5ghz cleanair config** command.

show ap dot11 5ghz cleanair config

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In Release 3.3SE, you can configure this command on the Mobility Agent (MA).

This example shows how to display the CleanAir configuration for 5-GHz band on the Mobility Controller:

```
Device# show ap dot11 5ghz cleanair config

CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
```

```
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 1
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Enabled
    CleanAir Driven RRM Sensitivity.............. : HIGH
    CleanAir Persistent Devices state............ : Enabled
```

This example shows how to display the CleanAir configuration for 5-GHz band on the Mobility Agent:

```
Device# show ap dot11 5ghz cleanair config

Mobility Controller Link Status.................. : UP
CleanAir Solution............................... : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
```

```
CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 5ghz cleanair device type

To display the 5-GHz interference devices, use the **show ap dot11 5ghz cleanair device type** command.

show ap dot11 5ghz cleanair device type {**all | canopy | cont-tx | dect-like | inv | jammer | nonstd | persistent | superag | tdd-tx | video | wimax-fixed | wimax-mobile**}

Syntax Description

all	Displays all CleanAir interferer devices for 5-GHz band.
canopy	Displays CleanAir interferers of type canopy for 5-GHz band.
cont-tx	Displays CleanAir interferers of type continuous transmitter for 5-GHz band.
dect-like	Displays CleanAir interferers of type Digital Enhanced Cordless Communication (DECT)-like phone for 5-GHz band.
inv	Displays CleanAir interferer devices using spectrally inverted WiFi signals for 5-GHz band.
jammer	Displays CleanAir interferers of type jammer for 5-GHz band.
nonstd	Displays CleanAir interferer devices using non-standard Wi-Fi channels for 5-GHz band.
persistent	Displays CleanAir persistent device interferers for 5-GHz band.
superag	Displays CleanAir interferers of type SuperAG for 5-GHz band.
tdd-tx	Displays CleanAir Time Division Duplex (TDD) transmitters for 5-GHz band.
video	Displays CleanAir interferers of type video camera for 5-GHz band.
winmax-fixed	Displays CleanAir interferers of type WiMax fixed for 5-GHz band.
wimax-mobile	Displays CleanAir interferers of type WiMax mobile for 5-GHz band.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Interference devices are listed only if there is an interference from any 5-GHz devices.

This example shows how to view all the 5-GHz interference devices:

```
Device# show ap dot11 5ghz cleanair device type all

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID

No    ClusterID          DevID  Type           AP Name                 ISI  RSSI  DC
Channel
-----------------------------------------------------------------------------------------------
```

show ap dot11 24ghz cleanair air-quality summary

To display the CleanAir AQ data for 2.4-GHz band, use the **show ap dot11 24ghz cleanair air-quality summary** command in user EXEC mode or privileged EXEC mode.

show ap dot11 24ghz cleanair air-quality summary

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the CleanAir AQ data for 2.4-GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality summary

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-------------------------------------------------------------
AP270ca.9b86.4546   1         99      99      0            No
AP2894.0f26.22df    6         98      97      0            No
AP2894.0f58.cc6b    11        99      99      0            No
AP2894.0f39.1040    6         97      97      0            No
AP2894.0f63.c6da    11        99      99      0            No
```

show ap dot11 24ghz cleanair air-quality worst

To display the worst air quality data for 2.4-GHz band, use the **show ap dot11 24ghz cleanair air-quality worst** command in user EXEC mode or privileged EXEC mode.

show ap dot11 24ghz cleanair air-quality worst

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the worst AQ data for 2.4-GHz band:

```
Device# show ap dot11 24ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection

AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
AP2895.0f39.1040    6         97      97      0            No
```

show ap dot11 24ghz cleanair config

To display the CleanAir configuration for 2.4-GHz band, use the **show ap dot11 24ghz cleanair config** command in user EXEC mode or privileged EXEC mode.

show ap dot11 24ghz cleanair config

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In Release 3.3SE, you can configure this command on the Mobility Agent (MA).

This example shows how to display the CleanAir configuration for 2.4-GHz band on the Mobility Controller:

```
Device# show ap dot11 24ghz cleanair config

CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 1
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Alarms................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State.............. : Enabled
    CleanAir Driven RRM Sensitivity.............. : HIGH
    CleanAir Persistent Devices state............ : Enabled
```

This example shows how to display the CleanAir configuration for 2.4-GHz band on the Mobility Agent:

```
Device# show ap dot11 24ghz cleanair config

Mobility Controller Link Status.................. : UP
CleanAir Solution................................ : Enabled
Air Quality Settings:
    Air Quality Reporting........................ : Enabled
    Air Quality Reporting Period (min)........... : 15
    Air Quality Alarms........................... : Enabled
    Air Quality Alarm Threshold.................. : 10
Interference Device Settings:
    Interference Device Reporting................ : Enabled
        TDD Transmitter.......................... : Enabled
        Jammer................................... : Enabled
        Continuous Transmitter................... : Enabled
        DECT-like Phone.......................... : Enabled
        Video Camera............................. : Enabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Enabled
        Canopy................................... : Enabled
        WiMax Mobile............................. : Enabled
        WiMax Fixed.............................. : Enabled
    Interference Device Types Triggering Alarms:
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
```

```
        Continuous Transmitter..................... : Disabled
        DECT-like Phone............................ : Disabled
        Video Camera............................... : Disabled
        WiFi Inverted.............................. : Enabled
        WiFi Invalid Channel....................... : Enabled
        SuperAG.................................... : Enabled
        Canopy..................................... : Disabled
        WiMax Mobile............................... : Disabled
        WiMax Fixed................................ : Disabled
    Interference Device Alarms..................... : Enabled
Additional CleanAir Settings:
    CleanAir Event-driven RRM State................ : Disabled
    CleanAir Driven RRM Sensitivity................ : LOW
    CleanAir Persistent Devices state.............. : Disabled
```

show ap dot11 24ghz cleanair summary

To display a summary of 2.4-GHz CleanAir devices, use the **show ap dot11 24ghz cleanair summary** command in user EXEC mode or privileged EXEC mode.

show ap dot11 24ghz cleanair summary

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This is an example of output from the **show ap dot11 24ghz cleanair summary** command:

```
Device# show ap dot11 24ghz cleanair summary

AP Name               MAC Address         Slot ID  Spectrum Capable  Spectrum Intelligence
   Spectrum Oper State
-----------------------------------------------------------------------------------------------------------
AP1cdf.0f95.1719      0817.35c7.1a60            0  Disabled          Disabled
   Down
AS-5508-5-AP3         0817.35dd.9f40            0  Disabled          Disabled
   Down
AP270ca.9b86.4546     0c85.259e.c350            0  Enabled           Enabled
   Up
AP2894.0f26.22df      0c85.25ab.cca0            0  Enabled           Enabled
   Up
AP2894.0f58.cc6b      0c85.25c7.b7a0            0  Enabled           Enabled
   Up
AP2894.0f39.1040      0c85.25de.2c10            0  Enabled           Enabled
   Up
AP2894.0f63.c6da      0c85.25de.c8e0            0  Enabled           Enabled
   Up
```

PART II

Flexible NetFlow Commands

- Flexible NetFlow Commands, page 41

CHAPTER 3

Flexible NetFlow Commands

- cache, page 42
- clear flow exporter, page 44
- clear flow monitor, page 45
- collect, page 46
- collect counter, page 47
- collect interface, page 48
- collect timestamp absolute, page 49
- collect transport tcp flags, page 50
- datalink flow monitor, page 51
- debug flow exporter, page 52
- debug flow monitor, page 53
- debug flow record, page 53
- debug sampler, page 54
- description, page 55
- destination, page 56
- dscp, page 57
- export-protocol netflow-v9, page 57
- exporter, page 58
- flow exporter, page 59
- flow monitor, page 60
- flow record, page 60
- ip flow monitor, page 61
- ipv6 flow monitor, page 62
- match datalink ethertype, page 64

- match datalink mac, page 65
- match datalink vlan, page 66
- match flow direction, page 66
- match interface, page 67
- match ipv4, page 68
- match ipv4 destination address, page 69
- match ipv4 source address, page 70
- match ipv4 ttl, page 71
- match ipv6, page 71
- match ipv6 destination address, page 72
- match ipv6 hop-limit, page 73
- match ipv6 source address, page 74
- match transport, page 74
- match transport icmp ipv4, page 75
- match transport icmp ipv6, page 76
- mode random 1 out-of, page 77
- option, page 78
- record, page 79
- sampler, page 80
- show flow exporter, page 81
- show flow interface, page 83
- show flow monitor, page 84
- show flow record, page 89
- show sampler, page 89
- source, page 91
- template data timeout, page 93
- transport, page 93
- ttl, page 94

cache

To configure a flow cache parameter for a flow monitor, use the **cache** command in flow monitor configuration mode. To remove a flow cache parameter for a flow monitor, use the **no** form of this command.

cache {**timeout** {**active**| **inactive**} *seconds*| **type normal**}

no cache {**timeout** {**active**| **inactive**} | **type**}

Syntax Description

timeout	Specifies the flow timeout.
active	Specifies the active flow timeout.
inactive	Specifies the inactive flow timeout.
seconds	The timeout value in seconds. The range is 1 to 604800 (7 days).
type	Specifies the type of the flow cache.
normal	Configures a normal cache type. The entries in the flow cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. This is the default cache type.

Command Default

The default flow monitor flow cache parameters are used.

The following flow cache parameters for a flow monitor are enabled:

- Cache type: normal
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 15 seconds

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Each flow monitor has a cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

The **cache timeout active** command controls the aging behavior of the normal type of cache. If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default, this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it. When you change the active flow timeout, the new timeout value takes effect immediately.

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout

is 15 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation. When you change the inactive flow timeout, the new timeout value takes effect immediately.

The **cache type normal** command specifies the normal cache type. This is the default cache type. The entries in the cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

To return a cache to its default settings, use the **default cache** flow monitor configuration command.

Note When a cache becomes full, new flows will not be monitored.

The following example shows how to configure the active timeout for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout active 4800
```

The following example shows how to configure the inactive timer for the flow monitor cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout inactive 30
```

The following example shows how to configure a normal cache:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache type normal
```

clear flow exporter

To clear the statistics for a Flexible NetFlow flow exporter, use the **clear flow exporter** command in privileged EXEC mode.

clear flow exporter [[**name**] *exporter-name*] **statistics**

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	Clears the flow exporter statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **clear flow exporter** command removes all statistics from the flow exporter. These statistics will not be exported and the data gathered in the cache will be lost.

You can view the flow exporter statistics by using the **show flow exporter statistics** privileged EXEC command.

The following example clears the statistics for all of the flow exporters configured on the device:

```
Device# clear flow exporter statistics
```

The following example clears the statistics for the flow exporter named FLOW-EXPORTER-1:

```
Device# clear flow exporter FLOW-EXPORTER-1 statistics
```

clear flow monitor

To clear a flow monitor cache or flow monitor statistics and to force the export of the data in the flow monitor cache, use the **clear flow monitor** command in privileged EXEC mode.

clear flow monitor [**name**] *monitor-name* [[**cache**] **force-export**| **statistics**]

Syntax Description

name	Specifies the name of a flow monitor.
monitor-name	Name of a flow monitor that was previously configured.
cache	(Optional) Clears the flow monitor cache information.
force-export	(Optional) Forces the export of the flow monitor cache statistics.
statistics	(Optional) Clears the flow monitor statistics.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **clear flow monitor cache** command removes all entries from the flow monitor cache. These entries will not be exported and the data gathered in the cache will be lost.

Note The statistics for the cleared cache entries are maintained.

The **clear flow monitor force-export** command removes all entries from the flow monitor cache and exports them using all flow exporters assigned to the flow monitor. This action can result in a short-term increase in CPU usage. Use this command with caution.

The **clear flow monitor statistics** command clears the statistics for this flow monitor.

Note The current entries statistic will not be cleared by the **clear flow monitor statistics** command because this is an indicator of how many entries are in the cache and the cache is not cleared with this command.

You can view the flow monitor statistics by using the **show flow monitor statistics** privileged EXEC command.

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1
```

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 force-export
```

The following example clears the cache for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Device# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

The following example clears the statistics for the flow monitor named FLOW-MONITOR-1:

```
Device# clear flow monitor name FLOW-MONITOR-1 statistics
```

collect

To configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record, use the **collect** command in flow record configuration mode.

collect {**counter**| **interface**| **timestamp**| **transport**}

Syntax Description

counter	Configures the number of bytes or packets in a flow as a non-key field for a flow record. For more information, see collect counter, on page 47.
interface	Configures the input and output interface name as a non-key field for a flow record. For more information, see collect interface, on page 48.
timestamp	Configures the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record. For more information, see collect timestamp absolute, on page 49.
transport	Enables the collecting of transport TCP flags from a flow record. For more information, see collect transport tcp flags, on page 50.

Command Default

Non-key fields are not configured for the flow monitor record.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

Note Although it is visible in the command-line help string, the **flow username** keyword is not supported.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter bytes long
```

collect counter

To configure the number of bytes or packets in a flow as a non-key field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a non-key field for a flow record, use the **no** form of this command.

collect counter {**bytes layer2 long**| **bytes long**| **packets long**}

no collect counter {**bytes layer2 long**| **bytes long**| **packets long**}

Syntax Description

bytes layer2 long	Configures the number of Layer 2 bytes seen in a flow as a non-key field, and enables collecting the total number of Layer 2 bytes from the flow using a 64-bit counter.
bytes long	Configures the number of bytes seen in a flow as a non-key field, and enables collecting the total number of bytes from the flow using a 64-bit counter.
packets long	Configures the number of packets seen in a flow as a non-key field and enables collecting the total number of packets from the flow using a 64-bit counter.

Command Default

The number of bytes or packets in a flow is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **collect counter bytes long** command configures a 64-bit counter for the number of bytes seen in a flow.

The **collect counter packets long** command configures a 64-bit counter that will be incremented for each packet seen in the flow. It is unlikely that a 64-bit counter will ever restart at 0.

To return this command to its default settings, use the **no collect counter** or **default collect counter** flow record configuration command.

The following example configures the total number of bytes in the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#collect counter bytes long
```

The following example configures the total number of packets from the flows as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect counter packets long
```

collect interface

To configure the input interface name as a non-key field for a flow record, use the **collect interface** command in flow record configuration mode. To disable the use of the input interface as a non-key field for a flow record, use the **no** form of this command.

collect interface input

no collect interface input

Syntax Description

input	Configures the input interface name as a non-key field and enables collecting the input interface from the flows.

Command Default

The input interface name is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

To return this command to its default settings, use the **no collect interface** or **default collect interface** flow record configuration command.

The following example configures the input interface as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect interface input
```

collect timestamp absolute

To configure the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **collect timestamp absolute** command in flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a non-key field for a flow record, use the **no** form of this command.

collect timestamp absolute {**first**| **last**}

no collect timestamp absolute {**first**| **last**}

Syntax Description

first	Configures the absolute time of the first seen packet in a flow as a non-key field and enables collecting time stamps from the flows.
last	Configures the absolute time of the last seen packet in a flow as a non-key field and enables collecting time stamps from the flows.

Command Default

The absolute time field is not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases the values for non-key fields are taken from only the first packet in the flow.

The following example configures time stamps based on the absolute time of the first seen packet in a flow as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute first
```

The following example configures time stamps based on the absolute time of the last seen packet in a flow as a non-key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect timestamp absolute last
```

collect transport tcp flags

To enable the collecting of transport TCP flags from a flow, use the **collect transport tcp flags** command in flow record configuration mode. To disable the collecting of transport TCP flags from the flow, use the **no** form of this command.

collect transport tcp flags

no collect transport tcp flags

Syntax Description

This command has no arguments or keywords.

Command Default

The transport layer fields are not configured as a non-key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The values of the transport layer fields are taken from all packets in the flow. You cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command. The following transport TCP flags are collected:

- **ack—**TCP acknowledgement flag
- **cwr—**TCP congestion window reduced flag

- **ece—**TCP ECN echo flag
- **fin—**TCP finish flag
- **psh—**TCP push flag
- **rst—**TCP reset flag
- **syn—**TCP synchronize flag
- **urg—**TCP urgent flag

To return this command to its default settings, use the **no collect collect transport tcp flags** or **default collect collect transport tcp flags** flow record configuration command.

The following example collects the TCP flags from a flow:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# collect transport tcp flags
```

datalink flow monitor

To apply a Flexible NetFlow flow monitor to an interface, use the **datalink flow monitor** command in interface configuration mode. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

no datalink flow monitor *monitor-name* **sampler** *sampler-name* **input**

Syntax Description

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	Enables the specified flow sampler for the flow monitor.
input	Monitors traffic that the switch receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you apply a flow monitor to an interface with the **datalink flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command and the flow sampler using the **sampler** global configuration command.

To enable a flow sampler for the flow monitor, you must have already created the sampler.

Note The **datalink flow monitor** command only monitors non-IPv4 and non-IPv6 traffic. To monitor IPv4 traffic, use the **ip flow monitor** command. To monitor IPv6 traffic, use the **ipv6 flow monitor** command.

This example shows how to enable Flexible NetFlow datalink monitoring on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# datalink flow monitor FLOW-MONITOR-1 sampler FLOW-SAMPLER-1 input
```

debug flow exporter

To enable debugging output for Flexible NetFlow flow exporters, use the **debug flow exporter** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow exporter [[**name**] *exporter-name*] [**error**| **event**| **packets** *number*]

no debug flow exporter [[**name**] *exporter-name*] [**error**| **event**| **packets** *number*]

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) The name of a flow exporter that was previously configured.
error	(Optional) Enables debugging for flow exporter errors.
event	(Optional) Enables debugging for flow exporter events.
packets	(Optional) Enables packet-level debugging for flow exporters.
number	(Optional) The number of packets to debug for packet-level debugging of flow exporters. The range is 1 to 65535.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example indicates that a flow exporter packet has been queued for process send:

```
Device# debug flow exporter
May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

debug flow monitor

To enable debugging output for Flexible NetFlow flow monitors, use the **debug flow monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow monitor [**error**| [**name**] *monitor-name* [**cache** [**error**]| **error**| **packets** *packets*]]

no debug flow monitor [**error**| [**name**] *monitor-name* [**cache** [**error**]| **error**| **packets** *packets*]]

Syntax Description

error	(Optional) Enables debugging for flow monitor errors for all flow monitors or for the specified flow monitor.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Enables debugging for the flow monitor cache.
cache error	(Optional) Enables debugging for flow monitor cache errors.
packets	(Optional) Enables packet-level debugging for flow monitors.
packets	(Optional) Number of packets to debug for packet-level debugging of flow monitors. The range is 1 to 65535.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example shows that the cache for FLOW-MONITOR-1 was deleted:

```
Device# debug flow monitor FLOW-MONITOR-1 cache
May 21 21:53:02.839: FLOW MON:  'FLOW-MONITOR-1' deleted cache
```

debug flow record

To enable debugging output for Flexible NetFlow flow records, use the **debug flow record** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow record [[**name**] *record-name*| **options** {**sampler-table**}| [**detailed**| **error**]]

no debug flow record [[**name**] *record-name*| **options** {**sampler-table**}| [**detailed**| **error**]]

Syntax Description

name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.
options	(Optional) Includes information on other flow record options.
sampler-table	(Optional) Includes information on the sampler tables.
detailed	(Optional) Displays detailed information.
error	(Optional) Displays errors only.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example enables debugging for the flow record:

```
Device# debug flow record FLOW-record-1
```

debug sampler

To enable debugging output for Flexible NetFlow samplers, use the **debug sampler** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sampler [**detailed**| **error**| [**name**] *sampler-name* [**detailed**| **error**| **sampling** *samples*]]

no debug sampler [**detailed**| **error**| [**name**] *sampler-name* [**detailed**| **error**| **sampling**]]

Syntax Description

detailed	(Optional) Enables detailed debugging for sampler elements.
error	(Optional) Enables debugging for sampler errors.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.
sampling *samples*	(Optional) Enables debugging for sampling and specifies the number of samples to debug.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following sample output shows that the debug process has obtained the ID for the sampler named SAMPLER-1:

```
Device# debug sampler detailed
*May 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,O)
 get ID succeeded:1
*May 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
 get ID succeeded:1
```

description

To configure a description for a flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*

no description *description*

Syntax Description

description	Text string that describes the flow monitor, flow exporter, or flow record.

Command Default

The default description for a flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To return this command to its default setting, use the **no description** or **default description** command in the appropriate configuration mode.

The following example configures a description for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# description Monitors traffic to 172.16.0.1 255.255.0.0
```

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a flow exporter, use the **no** form of this command.

destination {*hostname*| *ip-address*} **vrf** *vrf-label*

no destination {*hostname*| *ip-address*} **vrf** *vrf-label*

Syntax Description

hostname	Hostname of the device to which you want to send the NetFlow information.
ip-address	IPv4 address of the workstation to which you want to send the NetFlow information.
vrf	(Optional) Specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing and forwarding (VRF) instance for routing to the destination, instead of to the global routing table.
vrf-label	Name of the VRF instance.

Command Default

An export destination is not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IPv4 address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original Domain Name System (DNS) name resolution changes dynamically on the DNS server, the device does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data.

To return this command to its default setting, use the **no destination** or **default destination** command in flow exporter configuration mode.

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 10.0.0.4
```

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system using a VRF named VRF-1:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# destination 172.16.0.2 vrf VRF-1
```

dscp

To configure a differentiated services code point (DSCP) value for flow exporter datagrams, use the **dscp** command in flow exporter configuration mode. To remove a DSCP value for flow exporter datagrams, use the **no** form of this command.

dscp *dscp*

no dscp *dscp*

Syntax Description

dscp	DSCP to be used in the DSCP field in exported datagrams. The range is 0 to 63. The default is 0.

Command Default

The differentiated services code point (DSCP) value is 0.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To return this command to its default setting, use the **no dscp** or **default dscp** flow exporter configuration command.

The following example sets 22 as the value of the DSCP field in exported datagrams:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# dscp 22
```

export-protocol netflow-v9

To configure NetFlow Version 9 export as the export protocol for a Flexible NetFlow exporter, use the **export-protocol netflow-v9** command in flow exporter configuration mode.

export-protocol netflow-v9

Syntax Description

This command has no arguments or keywords.

Command Default

NetFlow Version 9 is enabled.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The device does not support NetFlow v5 export format, only NetFlow v9 export format is supported.

The following example configures NetFlow Version 9 export as the export protocol for a NetFlow exporter:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# export-protocol netflow-v9
```

exporter

To add a flow exporter for a flow monitor, use the **exporter** command in the appropriate configuration mode. To remove a flow exporter for a flow monitor, use the **no** form of this command.

exporter *exporter-name*

no exporter *exporter-name*

Syntax Description

exporter-name	Name of a flow exporter that was previously configured.

Command Default

An exporter is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must have already created a flow exporter by using the **flow exporter** command before you can apply the flow exporter to a flow monitor with the **exporter** command.

To return this command to its default settings, use the **no exporter** or **default exporter** flow monitor configuration command.

The following example configures an exporter for a flow monitor:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# exporter EXPORTER-1
```

flow exporter

To create a Flexible NetFlow flow exporter, or to modify an existing Flexible NetFlow flow exporter, and enter Flexible NetFlow flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a Flexible NetFlow flow exporter, use the **no** form of this command.

flow exporter *exporter-name*

no flow exporter *exporter-name*

Syntax Description

exporter-name	Name of the flow exporter that is being created or modified.

Command Default

Flexible NetFlow flow exporters are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters Flexible NetFlow flow exporter configuration mode:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)#
```

flow monitor

To create a flow monitor, or to modify an existing flow monitor, and enter flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a flow monitor, use the **no** form of this command.

flow monitor *monitor-name*

no flow monitor *monitor-name*

Syntax Description

monitor-name	Name of the flow monitor that is being created or modified.

Command Default

Flexible NetFlow flow monitors are not present in the configuration.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a flow record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the flow monitor's record and stored in the flow monitor cache.

The following example creates a flow monitor named FLOW-MONITOR-1 and enters flow monitor configuration mode:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)#
```

flow record

To create a Flexible NetFlow flow record, or to modify an existing Flexible NetFlow flow record, and enter Flexible NetFlow flow record configuration mode, use the **flow record** command in global configuration mode. To remove a Flexible NetFlow record, use the **no** form of this command.

flow record *record-name*

no flow record *record-name*

Syntax Description

record-name	Name of the flow record that is being created or modified.

Command Default

A Flexible NetFlow flow record is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record defines the keys that Flexible NetFlow uses to identify packets in the flow, as well as other fields of interest that Flexible NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters.

The following example creates a flow record named FLOW-RECORD-1, and enters Flexible NetFlow flow record configuration mode:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)#
```

ip flow monitor

To enable a Flexible NetFlow flow monitor for IPv4 traffic that the device is receiving, use the **ip flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ip flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

Syntax Description

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv4 traffic that the device receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to an interface with the **ip flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

ipv6 flow monitor

To enable a flow monitor for IPv6 traffic that the device is receiving, use the **ipv6 flow monitor** command in interface configuration mode. To disable a flow monitor, use the **no** form of this command.

ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] **input**

Syntax Description

monitor-name	Name of the flow monitor to apply to the interface.
sampler *sampler-name*	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv6 traffic that the device receives on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you can apply a flow monitor to the interface with the **ipv6 flow monitor** command, you must have already created the flow monitor using the **flow monitor** global configuration command.

When you add a sampler to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on the interface. You must first remove the flow monitor from the interface and then enable the same flow monitor with a sampler.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 100 sampler it is expected that the packet and byte counters will have to be multiplied by 100.

The following example enables a flow monitor for monitoring input traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

The following example shows how to remove a flow monitor from an interface so that it can be enabled with the sampler:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

match datalink ethertype

To configure the EtherType of the packet as a key field for a flow record, use the **match datalink ethertype** command in flow record configuration mode. To disable the EtherType of the packet as a key field for a flow record, use the **no** form of this command.

match datalink ethertype

no match datalink ethertype

Syntax Description

This command has no arguments or keywords.

Command Default

The EtherType of the packet is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

When you configure the EtherType of the packet as a key field for a flow record using the **match datalink ethertype** command, the traffic flow that is created is based on the type of flow monitor that is assigned to the interface:

- When a datalink flow monitor is assigned to an interface using the **datalink flow monitor** interface configuration command, it creates unique flows for different Layer 2 protocols.
- When an IP flow monitor is assigned to an interface using the **ip flow monitor** interface configuration command, it creates unique flows for different IPv4 protocols.
- When an IPv6 flow monitor is assigned to an interface using the **ipv6 flow monitor** interface configuration command, it creates unique flows for different IPv6 protocols.

To return this command to its default settings, use the **no match datalink ethertype** or **default match datalink ethertype** flow record configuration command.

The following example configures the EtherType of the packet as a key field for a Flexible NetFlow flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink ethertype
```

match datalink mac

To configure the use of MAC addresses as a key field for a flow record, use the **match datalink mac** command in flow record configuration mode. To disable the use of MAC addresses as a key field for a flow record, use the **no** form of this command.

match datalink mac {**destination address input**| **source address input**}

no match datalink mac {**destination address input**| **source address input**}

Syntax Description

destination address	Configures the use of the destination MAC address as a key field.
input	Specifies the MAC address of input packets.
source address	Configures the use of the source MAC address as a key field.

Command Default

MAC addresses are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **input** keyword is used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addresses in the network traffic.

Note When a datalink flow monitor is assigned to an interface or VLAN record, it creates flows only for non-IPv6 or non-IPv4 traffic.

To return this command to its default settings, use the **no match datalink mac** or **default match datalink mac** flow record configuration command.

The following example configures the use of the destination MAC address of packets that are received by the device as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink mac destination address input
```

match datalink vlan

To configure the VLAN ID as a key field for a flow record, use the **match datalink vlan** command in flow record configuration mode. To disable the use of the VLAN ID value as a key field for a flow record, use the **no** form of this command.

match datalink vlan input

no match datalink vlan input

Syntax Description

input	Configures the VLAN ID of traffic being received by the device as a key field.

Command Default

The VLAN ID is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **input** keyword is used to specify the observation point that is used by the **match datalink vlan** command to create flows based on the unique VLAN IDs in the network traffic.

The following example configures the VLAN ID of traffic being received by the device as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink vlan input
```

match flow direction

To configure the flow direction as key fields for a flow record, use the **match flow direction** command in flow record configuration mode. To disable the use of the flow direction as key fields for a flow record, use the **no** form of this command.

match flow direction

no match flow direction

Syntax Description

This command has no arguments or keywords.

Command Default

The flow direction is not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The **match flow direction** command captures the direction of the flow as a key field. This feature is most useful when a single flow monitor is configured for input and output flows. It can be used to find and eliminate flows that are being monitored twice, once on input and once on output. This command can help to match up pairs of flows in the exported data when the two flows are flowing in opposite directions.

The following example configures the direction the flow was monitored in as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow direction
```

match interface

To configure the input and output interfaces as key fields for a flow record, use the **match interface** command in flow record configuration mode. To disable the use of the input and output interfaces as key fields for a flow record, use the **no** form of this command.

match interface {**input**| **output**}

no match interface {**input**| **output**}

Syntax Description

input	Configures the input interface as a key field.
output	Configures the output interface as a key field.

Command Default

The input and output interfaces are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the input interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface input
```

The following example configures the output interface as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match interface output
```

match ipv4

To configure one or more of the IPv4 fields as a key field for a flow record, use the **match ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a flow record, use the **no** form of this command.

match ipv4 {**destination address**| **protocol**| **source address**| **tos**| **ttl**| **version**}

no match ipv4 {**destination address**| **protocol**| **source address**| **tos**| **ttl**| **version**}

Syntax Description

destination address	Configures the IPv4 destination address as a key field. For more information see match ipv4 destination address, on page 69.
protocol	Configures the IPv4 protocol as a key field.
source address	Configures the IPv4 destination address as a key field. For more information see match ipv4 source address, on page 70.
tos	Configures the IPv4 ToS as a key field.
ttl	Configures the IPv4 time-to-live (TTL) field as a key field for a flow record. For more information see match ipv4 ttl, on page 71.
version	Configures the IP version from IPv4 header as a key field.

Command Default

The use of one or more of the IPv4 fields as a key field for a user-defined flow record is not enabled.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv4 protocol as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 protocol
```

match ipv4 destination address

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination address** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a flow record, use the **no** form of this command.

match ipv4 destination address

no match ipv4 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 destination address** or **default match ipv4 destination address** flow record configuration command.

The following example configures the IPv4 destination address as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 destination address
```

match ipv4 source address

To configure the IPv4 source address as a key field for a flow record, use the **match ipv4 source address** command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a flow record, use the **no** form of this command.

match ipv4 source address

no match ipv4 source address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 source address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv4 source address** or **default match ipv4 source address** flow record configuration command.

The following example configures the IPv4 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 source address
```

match ipv4 ttl

To configure the IPv4 time-to-live (TTL) field as a key field for a flow record, use the **match ipv4 ttl** command in flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a flow record, use the **no** form of this command.

match ipv4 ttl

no match ipv4 ttl

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 time-to-live (TTL) field is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match ipv4 ttl** command.

The following example configures IPv4 TTL as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv4 ttl
```

match ipv6

To configure one or more of the IPv6 fields as a key field for a flow record, use the **match ipv6** command in flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a flow record, use the **no** form of this command.

match ipv6 {**destination address**| **hop-limit**| **protocol**| **source address**| **traffic-class**| **version**}

no match ipv6 {**destination address**| **hop-limit**| **protocol**| **source address**| **traffic-class**| **version**}

Syntax Description

destination address	Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 72.

hop-limit	Configures the IPv6 hop limit as a key field. For more information see match ipv6 hop-limit, on page 73.
protocol	Configures the IPv6 protocol as a key field.
source address	Configures the IPv4 destination address as a key field. For more information see match ipv6 source address, on page 74.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 protocol field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 protocol
```

match ipv6 destination address

To configure the IPv6 destination address as a key field for a flow record, use the **match ipv6 destination address** command in flow record configuration mode. To disable the IPv6 destination address as a key field for a flow record, use the **no** form of this command.

match ipv6 destination address

no match ipv6 destination address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 destination address** or **default match ipv6 destination address** flow record configuration command.

The following example configures the IPv6 destination address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 destination address
```

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a flow record, use the **match ipv6 hop-limit** command in flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a flow record, use the **no** form of this command.

match ipv6 hop-limit

no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined flow record is not enabled by default.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the hop limit of the packets in the flow as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 hop-limit
```

match ipv6 source address

To configure the IPv6 source address as a key field for a flow record, use the **match ipv6 source address** command in flow record configuration mode. To disable the use of the IPv6 source address as a key field for a flow record, use the **no** form of this command.

match ipv6 source address

no match ipv6 source address

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv6 source address is not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

To return this command to its default settings, use the **no match ipv6 source address** or **default match ipv6 source address** flow record configuration command.

The following example configures a IPv6 source address as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match ipv6 source address
```

match transport

To configure one or more of the transport fields as a key field for a flow record, use the **match transport** command in flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a flow record, use the **no** form of this command.

match transport {**destination-port**| **icmp ipv4**| **icmp ipv6**| **igmp type**| **source-port**}

no match transport {**destination-port**| **icmp ipv4**| **icmp ipv6**| **igmp type**| **source-port**}

Syntax Description

destination-port	Configures the transport destination port as a key field.
icmp ipv4	Configures the ICMP IPv4 type field and the code field as key fields. For more information see, match transport icmp ipv4, on page 75.
icmp ipv6	Configures the ICMP IPv6 type field and the code field as key fields. For more information see, match transport icmp ipv6, on page 76.
igmp type	Configures time stamps based on the system uptime as a key field.
source-port	Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the destination port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport source-port
```

match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a flow record, use the **match transport icmp ipv4** command in flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a flow record, use the **no** form of this command.

match transport icmp ipv4 {**code**| **type**}

no match transport icmp ipv4 {**code**| **type**}

Syntax Description

code	Configures the IPv4 ICMP code as a key field.
type	Configures the IPv4 ICMP type as a key field.

Command Default

The ICMP IPv4 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv4 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv4 type
```

match transport icmp ipv6

To configure the ICMP IPv6 type field and the code field as key fields for a flow record, use the **match transport icmp ipv6** command in flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a flow record, use the **no** form of this command.

match transport icmp ipv6 {**code**| **type**}

no match transport icmp ipv6 {**code**| **type**}

Syntax Description

code	Configures the IPv6 ICMP code as a key field.
type	Configures the IPv6 ICMP type as a key field.

Command Default

The ICMP IPv6 type field and the code field are not configured as key fields.

Command Modes

Flow record configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

The following example configures the IPv6 ICMP code field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match transport icmp ipv6 type
```

mode random 1 out-of

To enable random sampling and to specify the packet interval for a Flexible NetFlow sampler, use the **mode random 1 out-of** command in sampler configuration mode. To remove the packet interval information for a Flexible NetFlow sampler, use the **no** form of this command.

mode random 1 out-of *window-size*

no mode

Syntax Description

window-size	Specifies the window size from which to select packets. The range is 2 to 1024.

Command Default

The mode and the packet interval for a sampler are not configured.

Command Modes

Sampler configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **deterministic** keyword was removed.

Usage Guidelines

A total of four unique samplers are supported on the . Packets are chosen in a manner that should eliminate any bias from traffic patterns and counter any attempt by users to avoid monitoring.

Note The **deterministic** keyword is not supported, even though it is visible in the command-line help string.

The following example enables random sampling with a window size of 1000:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)# mode random 1 out-of 1000
```

option

To configure optional data parameters for a flow exporter for Flexible NetFlow, use the **option** command in flow exporter configuration mode. To remove optional data parameters for a flow exporter, use the **no** form of this command.

option {**exporter-stats**| **interface-table**| **sampler-table**} [**timeout** *seconds*]

no option {**exporter-stats**| **interface-table**| **sampler-table**}

Syntax Description

exporter-stats	Configures the exporter statistics option for flow exporters.
interface-table	Configures the interface table option for flow exporters.
sampler-table	Configures the export sampler table option for flow exporters.
timeout *seconds*	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.

Command Default

The timeout is 600 seconds. All other optional data parameters are not configured.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **application-table** and **usermac-table** keywords were added.

Usage Guidelines

The **option exporter-stats** command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows the collector to estimate packet loss for the export records it receives. The optional timeout alters the frequency at which the reports are sent.

The **option interface-table** command causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

The **option sampler-table** command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

To return this command to its default settings, use the **no option** or **default option** flow exporter configuration command.

The following example shows how to enable the periodic sending of the sampler option table, which allows the collector to map the sampler ID to the sampler type and rate:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option sampler-table
```

The following example shows how to enable the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option exporter-stats
```

The following example shows how to enable the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# option interface-table
```

record

To add a flow record for a Flexible NetFlow flow monitor, use the **record** command in flow monitor configuration mode. To remove a flow record for a Flexible NetFlow flow monitor, use the **no** form of this command.

record *record-name*

no record

Syntax Description

record-name	Name of a user-defined flow record that was previously configured.

Command Default

A flow record is not configured.

Command Modes

Flow monitor configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Each flow monitor requires a record to define the contents and layout of its cache entries. The flow monitor can use one of the wide range of predefined record formats, or advanced users may create their own record formats.

Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command for the flow monitor.

The following example configures the flow monitor to use FLOW-RECORD-1:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# record FLOW-RECORD-1
```

sampler

To create a Flexible NetFlow flow sampler, or to modify an existing Flexible NetFlow flow sampler, and to enter Flexible NetFlow sampler configuration mode, use the **sampler** command in global configuration mode. To remove a sampler, use the **no** form of this command.

sampler *sampler-name*

no sampler *sampler-name*

Syntax Description

sampler-name	Name of the flow sampler that is being created or modified.

Command Default

Flexible NetFlow flow samplers are not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Flow samplers are used to reduce the load placed by Flexible NetFlow on the networking device to monitor traffic by limiting the number of packets that are analyzed. You configure a rate of sampling that is 1 out of a range of 2-1024 packets. Flow samplers are applied to interfaces in conjunction with a flow monitor to implement sampled Flexible NetFlow.

To enable flow sampling, you configure the record that you want to use for traffic analysis and assign it to a flow monitor. When you apply a flow monitor with a sampler to an interface, the sampled packets are analyzed at the rate specified by the sampler and compared with the flow record associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

The following example creates a flow sampler name SAMPLER-1:

```
Device(config)# sampler SAMPLER-1
Device(config-sampler)#
```

show flow exporter

To display flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [**broker** [**detail**| **picture**]| **export-ids netflow-v9**| [**name**] *exporter-name* [**statistics**| **templates**]| **statistics**| **templates**]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow flow exporter.
detail	(Optional) Displays detailed information about the flow exporter broker.
picture	(Optional) Displays a picture of the broker state.
export-ids netflow-v9	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	(Optional) Displays statistics for all flow exporters or for the specified flow exporter.
templates	(Optional) Displays template information for all flow exporters or for the specified flow exporter.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter
Flow Exporter FLOW-EXPORTER-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 192.168.0.1
    Source IP address:      192.168.0.2
    Transport Protocol:     UDP
    Destination Port:       9995
    Source Port:            55864
    DSCP:                   0x0
    TTL:                    255
    Output Features:        Used
```

This table describes the significant fields shown in the display:

Table 6: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.

Field	Description
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the **output-features** command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

The following example displays the status and statistics for all of the flow exporters configured on a device:

```
Device# show flow exporter name FLOW-EXPORTER-1 statistics
Flow Exporter FLOW-EXPORTER-1:
  Packet send statistics (last cleared 2w6d ago):
    Successfully sent:         0                     (0 bytes)
```

show flow interface

To display the Flexible NetFlow configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description

type	(Optional) The type of interface on which you want to display Flexible NetFlow accounting configuration information.
number	(Optional) The number of the interface on which you want to display Flexible NetFlow accounting configuration information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example displays the Flexible NetFlow accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Device# show flow interface gigabitethernet1/0/1

Interface Ethernet1/0
        monitor:         FLOW-MONITOR-1
        direction:       Output
        traffic(ip):     on
Device# show flow interface gigabitethernet1/0/2
```

```
Interface Ethernet0/0
        monitor:         FLOW-MONITOR-1
        direction:       Input
        traffic(ip):     sampler SAMPLER-2#
```

The table below describes the significant fields shown in the display.

Table 7: show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: • on—The flow monitor is in normal mode. • sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

show flow monitor [**broker** [**detail**| **picture**]| [**name**] *monitor-name* [**cache** [**format** {**csv**| **record**| **table**}]]| **provisioning**| **statistics**]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the flow monitor
detail	(Optional) Displays detailed information about the flow monitor broker.

picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
provisioning	(Optional) Displays the flow monitor provisioning information.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that Flexible NetFlow uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which Flexible NetFlow collects values as additional data for the cache.

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 8: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

```
Device# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
```

```
IP TTL:                                 11
tcp flags:                              0x20
counter bytes long:                     132059538
counter packets long:                   1158417
```

This table describes the significant fields shown in the display.

Table 9: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
DATALINK MAC SOURCE ADDRESS INPUT	MAC source address of input packets.
DATALINK MAC DESTINATION ADDRESS INPUT	MAC destination address of input packets.
IPV6 SOURCE ADDRESS	IPv6 source address.
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.

Field	Description
counter packets	Number of packets that have been counted.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

```
Device# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                           Normal (Platform cache)
  Cache size:                          Unknown
  Current entries:                           1

  Flows added:                               3
  Flows aged:                                2
    - Active timeout      (   300 secs)      2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
===========================  ===========================  =============  =============
=============  =============  ==========  =======  ======  ======  =========  ==========
=========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
       1111           2222           6        6  0x05        11  0x20        132059538
1158417
```

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

The following example displays the status and statistics for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                                Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                                1

  Flows added:                                    3
  Flows aged:                                     2
    - Active timeout      (   300 secs)           2
```

show flow record

To display the status and statistics for a Flexible NetFlow flow record, use the **show flow record** command in privileged EXEC mode.

show flow record [**broker** [**detail**| **picture**]| [**name**] *record-name*]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow flow record.
detail	(Optional) Displays detailed information about the flow record broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example displays the status and statistics for FLOW-RECORD-1:

```
Device# show flow record FLOW-RECORD-1
flow record FLOW-RECORD-1:
  Description:        User defined
  No. of users:       0
  Total field space:  24 bytes
  Fields:
    match ipv6 destination address
    match transport source-port
    collect interface input
```

show sampler

To display the status and statistics for a Flexible NetFlow sampler, use the **show sampler** command in privileged EXEC mode.

show sampler [**broker** [**detail**| **picture**]| [**name**] *sampler-name*]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow sampler.
detail	(Optional) Displays detailed information about the sampler broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example displays the status and statistics for all of the flow samplers configured:

```
Device# show sampler
Sampler SAMPLER-1:
  ID:             2083940135
  export ID:      0
  Description:    User defined
  Type:           Invalid (not in use)
  Rate:           1 out of 32
  Samples:        0
  Requests:       0
  Users (0):

Sampler SAMPLER-2:
  ID:             3800923489
  export ID:      1
  Description:    User defined
  Type:           random
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
    flow monitor FLOW-MONITOR-1 (datalink,vlan1)  0 out of 0
```

This table describes the significant fields shown in the display.

Table 10: show sampler Field Descriptions

Field	Description
ID	ID number of the flow sampler.

Field	Description
Export ID	ID of the flow sampler export.
Description	Description that you configured for the flow sampler, or the default description User defined.
Type	Sampling mode that you configured for the flow sampler.
Rate	Window size (for packet selection) that you configured for the flow sampler. The range is 2 to 32768.
Samples	Number of packets sampled since the flow sampler was configured or the device was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. See the explanation of the Requests field in this table.
Requests	Number of times the flow sampler was queried to determine if the traffic needed to be sampled.
Users	Interfaces on which the flow sampler is configured.

source

To configure the source IP address interface for all of the packets sent by a Flexible NetFlow flow exporter, use the **source** command in flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a Flexible NetFlow flow exporter, use the **no** form of this command.

source *interface-type interface-number*

no source

Syntax Description

interface-type	Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.
interface-number	Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.

Command Default

The IP address of the interface over which the Flexible NetFlow datagram is transmitted is used as the source IP address.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The benefits of using a consistent IP source address for the datagrams that Flexible NetFlow sends include the following:

- The source IP address of the datagrams exported by Flexible NetFlow is used by the destination system to determine from which device the Flexible NetFlow data is arriving. If your network has two or more paths that can be used to send Flexible NetFlow datagrams from the device to the destination system and you do not specify the source interface from which the source IP address is to be obtained, the device uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive Flexible NetFlow datagrams from the same device, but with different source IP addresses. When the destination system receives Flexible NetFlow datagrams from the same device with different source IP addresses, the destination system treats the Flexible NetFlow datagrams as if they were being sent from different devices. To avoid having the destination system treat the Flexible NetFlow datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the Flexible NetFlow datagrams it receives from all of the possible source IP addresses in the device into a single Flexible NetFlow flow.
- If your device has multiple interfaces that can be used to transmit datagrams to the destination system, and you do not configure the **source** command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting Flexible NetFlow traffic. Creating and maintaining access lists for permitting Flexible NetFlow traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for Flexible NetFlow datagrams to a single IP address for each device that is exporting Flexible NetFlow traffic.

Caution The interface that you configure as the **source** interface must have an IP address configured, and it must be up.

Tip When a transient outage occurs on the interface that you configured with the **source** command, the Flexible NetFlow exporter reverts to the default behavior of using the IP address of the interface over which the datagrams are being transmitted as the source IP address for the datagrams. To avoid this problem, use a loopback interface as the source interface because loopback interfaces are not subject to the transient outages that can occur on physical interfaces.

To return this command to its default settings, use the **no source** or **default source** flow exporter configuration command.

The following example shows how to configure Flexible NetFlow to use a loopback interface as the source interface for NetFlow traffic:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# source loopback 0
```

template data timeout

To specify a timeout period for resending flow exporter template data, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a flow exporter, use the **no** form of this command.

template data timeout *seconds*

no template data timeout *seconds*

Syntax Description

seconds	Timeout value in seconds. The range is 1 to 86400. The default is 600.

Command Default

The default template resend timeout for a flow exporter is 600 seconds.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Flow exporter template data describes the exported data records. Data records cannot be decoded without the corresponding template. The **template data timeout** command controls how often those templates are exported.

To return this command to its default settings, use the **no template data timeout** or **default template data timeout** flow record exporter command.

The following example configures resending templates based on a timeout of 1000 seconds:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# template data timeout 1000
```

transport

To configure the transport protocol for a flow exporter for Flexible NetFlow, use the **transport** command in flow exporter configuration mode. To remove the transport protocol for a flow exporter, use the **no** form of this command.

transport udp *udp-port*

no transport udp *udp-port*

Syntax Description

udp *udp-port*	Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.

Command Default

Flow exporters use UDP on port 9995.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no transport** or **default transport flow exporter** configuration command.

The following example configures UDP as the transport protocol and a UDP port number of 250:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# transport udp 250
```

ttl

To configure the time-to-live (TTL) value, use the **ttl** command in flow exporter configuration mode. To remove the TTL value, use the **no** form of this command.

ttl *ttl*

no ttl *ttl*

Syntax Description

ttl	Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.

Command Default

Flow exporters use a TTL of 255.

Command Modes

Flow exporter configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To return this command to its default settings, use the **no ttl** or **default ttl** flow exporter configuration command.

The following example specifies a TTL of 15:

```
Device(config)# flow exporter FLOW-EXPORTER-1
Device(config-flow-exporter)# ttl 15
```

PART III

Interface and Hardware Components

- Interface and Hardware Commands, page 99

CHAPTER 4

Interface and Hardware Commands

- client vlan, page 101
- debug ilpower, page 102
- debug interface, page 103
- debug lldp packets, page 104
- debug nmsp, page 105
- debug platform poe, page 106
- duplex, page 106
- errdisable detect cause, page 108
- errdisable recovery cause, page 110
- errdisable recovery interval, page 112
- interface, page 113
- interface range, page 114
- ip mtu, page 115
- ipv6 mtu, page 116
- lldp (interface configuration), page 117
- logging event power-inline-status, page 118
- mdix auto, page 119
- mode (power-stack configuration), page 120
- network-policy, page 121
- network-policy profile (global configuration), page 122
- nmsp attachment suppress, page 123
- power efficient-ethernet auto, page 124
- power-priority , page 124
- power inline, page 126

- power inline police, page 129
- power supply, page 131
- show CAPWAP summary, page 132
- show controllers cpu-interface, page 133
- show controllers ethernet-controller, page 134
- show controllers utilization, page 143
- show eee, page 144
- show env, page 147
- show errdisable detect, page 150
- show errdisable recovery, page 151
- show interfaces, page 152
- show interfaces counters, page 156
- show interfaces switchport, page 158
- show interfaces transceiver, page 160
- show memory platform, page 162
- show module, page 164
- show mgmt-infra trace messages ilpower, page 165
- show mgmt-infra trace messages ilpower-ha, page 166
- show mgmt-infra trace messages platform-mgr-poe, page 166
- show network-policy profile, page 167
- show platform CAPWAP summary, page 168
- show platform forward, page 169
- show platform hardware fed switch forward, page 170
- show platform resources, page 172
- show platform software ilpower, page 173
- show platform software process list, page 174
- show platform software process slot switch, page 176
- show platform software status control-processor, page 178
- show processes cpu platform monitor, page 181
- show processes memory platform, page 182
- show power inline, page 185
- show stack-power , page 190
- show stack-power , page 192

- show system mtu, page 192
- show tech-support , page 193
- show wireless interface summary, page 195
- speed, page 195
- stack-power , page 197
- switchport block, page 198
- system mtu, page 199
- test mcu read-register, page 200
- voice-signaling vlan (network-policy configuration), page 202
- voice vlan (network-policy configuration), page 203
- wireless ap-manager interface, page 204
- wireless exclusionlist, page 205
- wireless linktest, page 206
- wireless management interface, page 207
- wireless peer-blocking forward-upstream, page 207

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*

no client vlan

Syntax Description

interface-id-name-or-group-name	Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

debug ilpower

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug ilpower {**cdp**| **controller**| **event**| **ha**| **ipc**| **police**| **port**| **powerman**| **registries**| **scp** | **sense**| **upoe**}

no debug ilpower {**cdp**| **controller**| **event**| **ha**| **ipc**| **police**| **port**| **powerman**| **registries**| **scp** | **sense**| **upoe**}

Syntax Description

cdp	Displays PoE Cisco Discovery Protocol (CDP) debug messages.
controller	Displays PoE controller debug messages.
event	Displays PoE event debug messages.
ha	Displays PoE high-availability messages.
ipc	Displays PoE Inter-Process Communication (IPC) debug messages.
police	Displays PoE police debug messages.
port	Displays PoE port manager debug messages.
powerman	Displays PoE power management debug messages.
registries	Displays PoE registries debug messages.
scp	Displays PoE SCP debug messages.
sense	Displays PoE sense debug messages.

upoe	Displays Cisco UPOE debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **upoe** keyword was added.

Usage Guidelines

This command is supported only on PoE-capable switches.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

debug interface

To enable debugging of interface-related activities, use the **debug interface** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**}| **states**}

no debug interface {*interface-id*| **counters** {**exceptions**| **protocol memory**}| **states**}

Syntax Description

interface-id	ID of the physical interface. Displays debug messages for the specified physical port, identified by type switch number/module number/port, for example, gigabitethernet 1/0/2.
counters	Displays counters debugging information.
exceptions	Displays debug messages when a recoverable exceptional condition occurs during the computation of the interface packet and data rate statistics.
protocol memory	Displays debug messages for memory operations of protocol counters.
states	Displays intermediary debug messages when an interface's state transitions.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

debug lldp packets

To enable debugging of Link Layer Discovery Protocol (LLDP) packets, use the **debug lldp packets** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug lldp packets

no debug lldp packets

Syntax Description This command has no arguments or keywords.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The **undebug lldp packets** command is the same as the **no debug lldp packets** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command.

debug nmsp

To enable debugging of the Network Mobility Services Protocol (NMSP) on the switch, use the **debug nmsp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug nmsp {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

no debug nmsp {**all**| **connection**| **detail**| **error**| **event**| **message** {**rx**| **tx**}| **packet**} [**switch** *switch-number*]

Syntax Description

all	Displays all NMSP debug messages.
connection	Displays debug messages for NMSP connection events.
detail	Displays detailed debug messages for NMSP.
error	Displays debugging information for NMSP error messages.
event	Displays debug messages for NMSP events.
message	Displays debugging information for NMSP messages.
rx	Displays debugging information for NMSP receive messages.
tx	Displays debugging information for NMSP transmit messages.
packet	Displays debug messages for NMSP packet events.
switch *switch-number*	(Optional) Specifies the switch number for which to display NMSP debugging information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

The **undebug nmsp** command is the same as the **no debug nmsp** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

debug platform poe

To enable debugging of a Power over Ethernet (PoE) port, use the **debug platform poe** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform poe [**error**| **info**] [**switch** *switch-number*]

no debug platform poe [**error**| **info**] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays PoE-related error debug messages.
info	(Optional) Displays PoE-related information debug messages.
switch *switch-number*	(Optional) Specifies the stack member. This keyword is supported only on stacking-capable switches.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform poe** command is the same as the **no debug platform poe** command.

duplex

To specify the duplex mode of operation for a port, use the **duplex** command in interface configuration mode. To return to the default value, use the **no** form of this command.

duplex {**auto**| **full**| **half**}

no duplex {**auto**| **full**| **half**}

Syntax Description

auto	Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
full	Enables full-duplex mode.
half	Enables half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

Command Default

The default is **auto** for Gigabit Ethernet ports.

You cannot configure the duplex mode on 10-Gigabit Ethernet ports; it is always **full**.

Duplex options are not supported on the 1000BASE-*x* or 10GBASE-*x* (where -*x* is -BX, -CWDM, -LX, -SX, or -ZX) small form-factor pluggable (SFP) modules.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

Note Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. How this command is applied depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces, and use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

You can verify your setting by entering the **show interfaces** privileged EXEC command.

This example shows how to configure an interface for full-duplex operation:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# duplex full
```

errdisable detect cause

To enable error-disable detection for a specific cause or for all causes, use the **errdisable detect cause** command in global configuration mode. To disable the error-disable detection feature, use the **no** form of this command.

errdisable detect cause {**all**| **arp-inspection**| **bpduguard shutdown vlan**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **pagp-flap**| **pppoe-ia-rate-limit** | **security-violation shutdown vlan**| **sfp-config-mismatch**}

no errdisable detect cause {**all**| **arp-inspection**| **bpduguard shutdown vlan**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **pagp-flap**| **pppoe-ia-rate-limit** | **security-violation shutdown vlan**| **sfp-config-mismatch**}

Syntax Description

all	Enables error detection for all error-disabled causes.
arp-inspection	Enables error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard shutdown vlan	Enables per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Enables error detection for DHCP snooping.
dtp-flap	Enables error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module. **Note** This error refers to an invalid small form-factor pluggable (SFP) module.
inline-power	Enables error detection for the Power over Ethernet (PoE) error-disabled cause. **Note** This keyword is supported only on switches with PoE ports.
l2ptguard	Enables error detection for a Layer 2 protocol-tunnel error-disabled cause.

link-flap	Enables error detection for link-state flapping.
loopback	Enables error detection for detected loopbacks.
pagp-flap	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
pppoe-ia-rate-limit	Enables error detection for the PPPoE Intermediate Agent rate-limit error-disabled cause.
security-violation shutdown vlan	Enables voice aware 802.1x security.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.

Command Default

Detection is enabled for all causes. All causes, except per-VLAN error disabling, are configured to shut down the entire port.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A cause (such as a link-flap or dhcp-rate-limit) is the reason for the error-disabled state. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the bridge protocol data unit (BPDU) guard, voice-aware 802.1x security, and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

```
Device(config)# errdisable detect cause link-flap
```

This command shows how to globally configure BPDU guard for a per-VLAN error-disabled state:

```
Device(config)# errdisable detect cause bpduguard shutdown vlan
```

This command shows how to globally configure voice-aware 802.1x security for a per-VLAN error-disabled state:

```
Device(config)# errdisable detect cause security-violation shutdown vlan
```

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

errdisable recovery cause

To enable the error-disabled mechanism to recover from a specific cause, use the **errdisable recovery cause** command in global configuration mode. To return to the default setting, use the **no** form of this command.

errdisable recovery cause {**all**| **arp-inspection**| **bpduguard**| **channel-misconfig**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **mac-limit**| **pagp-flap**| **port-mode-failure**| **pppoe-ia-rate-limit**| **psecure-violation**| **security-violation**| **sfp-config-mismatch**| **storm-control**| **udld**| **vmps**}

no errdisable recovery cause {**all**| **arp-inspection**| **bpduguard**| **channel-misconfig**| **dhcp-rate-limit**| **dtp-flap**| **gbic-invalid**| **inline-power**| **l2ptguard**| **link-flap**| **loopback**| **mac-limit**| **pagp-flap**| **port-mode-failure**| **pppoe-ia-rate-limit**| **psecure-violation**| **security-violation**| **sfp-config-mismatch**| **storm-control**| **udld**| **vmps**}

Syntax Description

all	Enables the timer to recover from all error-disabled causes.
arp-inspection	Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.
bpduguard	Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
dhcp-rate-limit	Enables the timer to recover from the DHCP snooping error-disabled state.
dtp-flap	Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
gbic-invalid	Enables the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. **Note** This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
inline-power	Enables the timer to recover from the Power over Ethernet (PoE) error-disabled state. This keyword is supported only on switches with PoE ports.
l2ptguard	Enables the timer to recover from a Layer 2 protocol tunnel error-disabled state.

link-flap	Enables the timer to recover from the link-flap error-disabled state.
loopback	Enables the timer to recover from a loopback error-disabled state.
mac-limit	Enables the timer to recover from the mac limit error-disabled state.
pagp-flap	Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
vmps	Enables the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state.

Command Default

Recovery is disabled for all causes.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A cause (such as all or BDPU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you do not enable the recovery for the cause, the interface stays in the error-disabled state until you enter the **shutdown** and the **no shutdown** interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

This example shows how to enable the recovery timer for the BPDU guard error-disabled cause:

```
Device(config)# errdisable recovery cause bpduguard
```

errdisable recovery interval

To specify the time to recover from an error-disabled state, use the **errdisable recovery interval** command in global configuration mode. To return to the default setting, use the **no** form of this command.

errdisable recovery interval *timer-interval*

no errdisable recovery interval *timer-interval*

Syntax Description

timer-interval	Time to recover from the error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.

Command Default

The default recovery interval is 300 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval.

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

This example shows how to set the timer to 500 seconds:

```
Device(config)# errdisable recovery interval 500
```

interface

To configure an interface, use the **interface** command.

interface {**Auto-Template** *Auto-Template interface-number*| **Capwap** *Capwap interface-number* | **Gigabit Ethernet** *Gigabit Ethernet interface number*| **Group VI** *Group VI interface number* **Internal Interface** *Internal Interface number* **Loopback** *Loopback interface number* **Null** *Null interface* **Port-channel** *interface number***Port-channel** *interface number* **TenGigabit Ethernet** *interface number* **Tunnel** *interface number* **Vlan** *interface number*}

Syntax Description

Auto-Template *Auto-template interface-number*	Enables you to configure auto-template interface. Values range from 1 to 999.
Capwap *Capwap interface number*	Enables you to configure CAPWAP tunnel interface. Values range from 0 to 2147483647.
GigabitEthernet *Gigabit Ethernet interface number*	Enables you to configure Gigabit Ethernet IEEE 802.3z interface. Values range from 0 to 9.
Group VI *Group VI interface number*	Enables you to configure the internal interface. Values range from 0 to 9.
Internal Interface Internal Interface	Enables you to configure internal interface.
Loopback *Loopback Interface number*	Enables you to configure loopback interface. Values range from 0 to 2147483647.
Null *Null interface number*	Enables you to configure null interface. Value is 0.
Port-channel *interface number*	Enables you to configure Ethernet channel interfaces. Values range from 1 to 128.
TenGigabitEthernet *interface number*	Enables you to configure a 10-Gigabit Ethernet interface. Values range from 0 to 9.
Tunnel *interface number*	Enables you to configure the tunnel interface. Values range from 0 to 2147483647.
Vlan *interface number*	Enables you to configure switch VLAN interfaces. Values range from 0 to 4098.

Command Default

None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines You can not use the "no" form of this command.

This example shows how you can configure interface:

```
Device# interface Tunnel 15
```

interface range

To configure an interface range, use the **interface range** command.

interface range {**Gigabit Ethernet** *interface-number* | **Loopback** *interface-number* | **Port Channel** *interface-number* | **TenGigabit Ethernet** *interface-number* **Tunnel** *interface-number* **Vlan** *interface-number* **Macro** *WORD*}

Syntax Description

GigabitEthernet *interface-number*	Configures the Gigabit Ethernet IEEE 802.3z interface. Values range from 1 to 9.
Loopback *interface-number*	Configures the loopback interface. Values range from 0 to 2147483647.
Port-Channel *interface-number*	Configures 10-Gigabit Ethernet channel of interfaces. Values range from 1 to 128.
TenGigabit Ethernet *interface-number*	Configures 10-Gigabit Ethernet interfaces. Values range from 0 to 9.
Tunnel *interface-number*	Configures the tunnel interface. Values range from 0 to 2147483647.
VLAN *interface-number*	Configures the switch VLAN interfaces. Values range from 1 to 4095.
Macro *WORD*	Configures the keywords to interfaces. Support up to 32 characters.

Command Default None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how you can configure interface range:

```
Device(config)# interface range vlan 1
```

ip mtu

To set the IP maximum transmission unit (MTU) size of routed packets on all routed ports of the switch or switch stack, use the **ip mtu** command in interface configuration mode. To restore the default IP MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu *bytes*

Syntax Description

bytes	MTU size, in bytes. The range is from 68 up to the system MTU value (in bytes).

Command Default

The default IP MTU size for frames received and sent on all switch interfaces is 1500 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The upper limit of the IP value is based on the switch or switch stack configuration and refers to the currently applied system MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command.

To return to the default IP MTU setting, you can apply the **default ip mtu** command or the **no ip mtu** command on the interface.

You can verify your setting by entering the **show ip interface** *interface-id* or **show interfaces** *interface-id* privileged EXEC command.

The following example sets the maximum IP packet size for VLAN 200 to 1000 bytes:

```
Device(config)# interface vlan 200
Device(config-if)# ip mtu 1000
```

The following example sets the maximum IP packet size for VLAN 200 to the default setting of 1500 bytes:

```
Device(config)# interface vlan 200
Device(config-if)# default ip mtu
```

This is an example of partial output from the **show ip interface** *interface-id* command. It displays the current IP MTU setting for the interface.

```
Device# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

ipv6 mtu

To set the IPv6 maximum transmission unit (MTU) size of routed packets on all routed ports of the switch or switch stack, use the **ipv6 mtu** command in interface configuration mode. To restore the default IPv6 MTU size, use the **no** form of this command.

ipv6 mtu *bytes*

no ipv6 mtu *bytes*

Syntax Description

bytes	MTU size, in bytes. The range is from 1280 up to the system MTU value (in bytes).

Command Default

The default IPv6 MTU size for frames received and sent on all switch interfaces is 1500 bytes.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The upper limit of the IPv6 MTU value is based on the switch or switch stack configuration and refers to the currently applied system MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command.

To return to the default IPv6 MTU setting, you can apply the **default ipv6 mtu** command or the **no ipv6 mtu** command on the interface.

You can verify your setting by entering the **show ipv6 interface** *interface-id* or **show interface** *interface-id* privileged EXEC command.

The following example sets the maximum IPv6 packet size for an interface to 2000 bytes:

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# ipv6 mtu 2000
```

The following example sets the maximum IPv6 packet size for an interface to the default setting of 1500 bytes:

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# default ipv6 mtu
```

This is an example of partial output from the **show ipv6 interface** *interface-id* command. It displays the current IPv6 MTU setting for the interface.

```
Device# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set

<output truncated>
```

lldp (interface configuration)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

lldp {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

no lldp {**med-tlv-select** *tlv*| **receive**| **tlv-select power-management**| **transmit**}

Syntax Description

med-tlv-select	Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
tlv	String that identifies the TLV element. Valid values are the following: • **inventory-management—** LLDP MED Inventory Management TLV. • **location—** LLDP MED Location TLV. • **network-policy—** LLDP MED Network Policy TLV. • **power-management—** LLDP MED Power Management TLV.
receive	Enables the interface to receive LLDP transmissions.
tlv-select	Selects the LLDP TLVs to send.
power-management	Sends the LLDP Power Management TLV.
transmit	Enables LLDP transmission on the interface.

Command Default LLDP is enabled on supported interfaces.

Command Modes Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines This command is supported on 802.1 media types.

If the interface is configured as a tunnel port, LLDP is automatically disabled.

The following example shows how to disable LLDP transmission on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no lldp transmit
```

The following example shows how to enable LLDP transmission on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# lldp transmit
```

logging event power-inline-status

To enable the logging of Power over Ethernet (PoE) events, use the **logging event power-inline-status** command in interface configuration mode. To disable the logging of PoE status events, use the **no** form of this command.

logging event power-inline-status

no logging event power-inline-status

Syntax Description This command has no arguments or keywords.

Command Default Logging of PoE events is enabled.

Command Modes Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no** form of this command does not disable PoE error events.

This example shows how to enable logging of PoE events on a port:

```
Device(config-if)# interface gigabitethernet1/0/1
Device(config-if)# logging event power-inline-status
Device(config-if)#
```

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command in interface configuration mode. To disable auto-MDIX, use the **no** form of this command.

mdix auto

no mdix auto

Syntax Description

This command has no arguments or keywords.

Command Default

Auto-MDIX is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.

When you enable auto-MDIX on an interface, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed and duplex) is enabled on one or both of the connected interfaces, link up occurs, even if the cable type (straight-through or crossover) is incorrect.

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller** *interface-id* **phy** privileged EXEC command.

This example shows how to enable auto-MDIX on a port:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto
Device(config-if)# duplex auto
Device(config-if)# mdix auto
```

```
Device(config-if)# end
```

mode (power-stack configuration)

To configure power stack mode for the power stack, use the **mode** command in power-stack configuration mode. To return to the default settings, use the **no** form of the command.

mode {**power-shared**| **redundant**} **[strict]**

no mode

Syntax Description

power-shared	Sets the power stack to operate in power-shared mode. This is the default.
redundant	Sets the power stack to operate in redundant mode. The largest power supply is removed from the power pool to be used as backup power in case one of the other power supplies fails.
strict	(Optional) Configures the power stack mode to run a strict power budget. The stack power needs cannot exceed the available power.

Command Default

The default modes are **power-shared** and nonstrict.

Command Modes

Power-stack configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is available only on switch stacks running the IP Base or IP Services feature set.

To access power-stack configuration mode, enter the **stack-power stack** *power stack name* global configuration command.

Entering the **no mode** command sets the switch to the defaults of **power-shared** and non-strict mode.

Note For stack power, available power is the total power available for PoE from all power supplies in the power stack, available power is the power allocated to all powered devices connected to PoE ports in the stack, and consumed power is the actual power consumed by the powered devices.

In **power-shared** mode, all of the input power can be used for loads, and the total available power appears as one large power supply. The power budget includes all power from all supplies. No power is set aside for

power supply failures. If a power supply fails, load shedding (shutting down of powered devices or switches) might occur.

In **redundant** mode, the largest power supply is removed from the power pool to use as backup power in case one of the other power supplies fails. The available power budget is the total power minus the largest power supply. This reduces the available power in the pool for switches and powered devices, but in case of a failure or an extreme power load, there is less chance of having to shut down switches or powered devices.

In **strict** mode, when a power supply fails and the available power drops below the budgeted power, the system balances the budget through load shedding of powered devices, even if the actual power is less than the available power. In nonstrict mode, the power stack can run in an over-allocated state and is stable as long as the actual power does not exceed the available power. In this mode, a powered device drawing more than normal power could cause the power stack to start shedding loads. This is normally not a problem because most devices do not run at full power. The chances of multiple powered devices in the stack requiring maximum power at the same time is small.

In both strict and nonstrict modes, power is denied when there is no power available in the power budget.

This is an example of setting the power stack mode for the stack named power1 to power-shared with strict power budgeting. All power in the stack is shared, but when the total available power is allotted, no more devices are allowed power.

```
Device(config)# stack-power stack power1
Device(config-stackpower)# mode power-shared strict
Device(config-stackpower)# exit
```

This is an example of setting the power stack mode for the stack named power2 to redundant. The largest power supply in the stack is removed from the power pool to provide redundancy in case one of the other supplies fails.

```
Device(config)# stack-power stack power2
Device(config-stackpower)# mode redundant
Device(config-stackpower)# exit
```

network-policy

To apply a network-policy profile to an interface, use the **network-policy** command in interface configuration mode. To remove the policy, use the **no** form of this command.

network-policy *profile-number*

no network-policy

Syntax Description

profile-number	The network-policy profile number to apply to the interface.

Command Default

No network-policy profiles are applied.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy** *profile number* interface configuration command to apply a profile to an interface.

You cannot apply the **switchport voice vlan** command on an interface if you first configure a network-policy profile on it. However, if **switchport voice vlan** *vlan-id* is already configured on the interface, you can apply a network-policy profile on the interface. The interface then has the voice or voice-signaling VLAN network-policy profile applied.

This example shows how to apply network-policy profile 60 to an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# network-policy 60
```

network-policy profile (global configuration)

To create a network-policy profile and to enter network-policy configuration mode, use the **network-policy profile** command in global configuration mode. To delete the policy and to return to global configuration mode, use the **no** form of this command.

network-policy profile *profile-number*

no network-policy profile *profile-number*

Syntax Description

profile-number	Network-policy profile number. The range is 1 to 4294967295.

Command Default

No network-policy profiles are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

When you are in network-policy profile configuration mode, you can create the profile for voice and voice signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

This example shows how to create network-policy profile 60:

```
Device(config)# network-policy profile 60
Device(config-network-policy)#
```

nmsp attachment suppress

To suppress the reporting of attachment information from a specified interface, use the **nmsp attachment suppress** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

nmsp attachment suppress

no nmsp attachment suppress

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **nmsp attachment suppress** interface configuration command to configure an interface to not send location and attachment notifications to a Cisco Mobility Services Engine (MSE).

Note Attachment information is not supported in Cisco IOS XE Denali 16.1.1 and later releases.

This example shows how to configure an interface to not send attachment information to the MSE:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# nmsp attachment suppress
```

power efficient-ethernet auto

To enable Energy Efficient Ethernet (EEE) for an interface, use the **power efficient-ethernet auto** command in interface configuration mode. To disable EEE on an interface, use the **no** form of this command.

power efficient-ethernet auto

no power efficient-ethernet auto

Syntax Description

This command has no arguments or keywords.

Command Default

EEE is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

The **power efficient-ethernet auto** command is available only if the interface is EEE capable. To check if an interface is EEE capable, use the **show eee capabilities** EXEC command.

When EEE is enabled, the device advertises and autonegotiates EEE to its link partner. To view the current EEE status for an interface, use the **show eee status** EXEC command.

This command does not require a license.

This example shows how to enable EEE for an interface:

```
Device(config-if)# power efficient-ethernet auto
Device(config-if)#
```

This example shows how to disable EEE for an interface:

```
Device(config-if)# no power efficient-ethernet auto
Device(config-if)#
```

power-priority

To configure Cisco StackPower power-priority values for a switch in a power stack and for its high-priority and low-priority PoE ports, use the **power-priority** command in switch stack-power configuration mode. To return to the default setting, use the **no** form of the command.

power-priority {**high** *value*| **low** *value*| **switch** *value*}

no power-priority {**high**| **low**| **switch**}

Syntax Description

high *value*	Sets the power priority for the ports configured as high-priority ports. The range is 1 to 27, with 1 as the highest priority. The **high** value must be lower than the value set for the low-priority ports and higher than the value set for the switch.
low *value*	Sets the power priority for the ports configured as low-priority ports. The range is 1 to 27. The **low** value must be higher than the value set for the high-priority ports and the value set for the switch.
switch *value*	Sets the power priority for the switch. The range is 1 to 27. The **switch** value must be lower than the values set for the low and high-priority ports.

Command Default

If no values are configured, the power stack randomly determines a default priority.

The default ranges are 1 to 9 for switches, 10 to 18 for high-priority ports, 19 to 27 for low-priority ports.

On non-PoE switches, the high and low values (for port priority) have no effect.

Command Modes

Switch stack-power configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To access switch stack-power configuration mode, enter the **stack-power switch** *switch-number* global configuration command.

Cisco StackPower power-priority values determine the order for shutting down switches and ports when power is lost and load shedding must occur. Priority values are from 1 to 27; the highest numbers are shut down first.

We recommend that you configure different priority values for each switch and for its high priority ports and low priority ports to limit the number of devices shut down at one time during a loss of power. If you try to configure the same priority value on different switches in a power stack, the configuration is allowed, but you receive a warning message.

Note This command is available only on switch stacks running the IP Base or IP Services feature set.

This is an example of setting the power priority for switch 1 in power stack a to 7, for the high-priority ports to 11, and for the low-priority ports to 20.

```
Device(config)# stack-power switch 1
Device(config-switch-stackpower)# stack-id power_stack_a
Device(config-switch-stackpower)# power-priority high 11
```

```
Device(config-switch-stackpower)# power-priority low 20
Device(config-switch-stackpower)# power-priority switch 7
Device(config-switch-stackpower)# exit
```

power inline

To configure the power management mode on Power over Ethernet (PoE) ports, use the **power inline** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

power inline {**auto** [**max** *max-wattage*]| **four-pair forced**| **never**| **port priority** {**high** | **low**} | **static** [**max** *max-wattage*]}

no power inline {**auto**| **four-pair forced**| **never**| **port priority** {**high** | **low**}| **static** [**max** *max-wattage*]}

Syntax Description

auto	Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. Allocation is first-come, first-serve.
max *max-wattage*	(Optional) Limits the power allowed on the port. The range is 4000 to 30000 mW. If no value is specified, the maximum is allowed.
four-pair forced	(Optional) Enable Four-pair PoE without L2 negotiation (Cisco UPOE switches only).
never	Disables device detection, and disables power to the port.
port	Configures the power priority of the port. The default priority is low.
priority {**high**|**low**}	Sets the power priority of the port. In case of a power supply failure, ports configured as low priority are turned off first and ports configured as high priority are turned off last. The default priority is low.
static	Enables powered-device detection. Pre-allocates (reserves) power for a port before the switch discovers the powered device. This action guarantees that the device connected to the interface receives enough power.

Command Default

The default is **auto** (enabled).

The maximum wattage is 30,000 mW.

The default port priority is low.

Command Default

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **four-pair forced** keywords were added.

Usage Guidelines

This command is supported only on PoE-capable ports. If you enter this command on a port that does not support PoE, this error message appears:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                 ^
% Invalid input detected at '^' marker.
```

In a switch stack, this command is supported on all ports in the stack that support PoE.

Cisco Universal Power Over Ethernet (Cisco UPOE) is a Cisco proprietary technology that extends the IEEE 802.at PoE standard to provide the capability to source up to 60 W of power over standard Ethernet cabling infrastructure (Class D or better) by using the spare pair of an RJ-45 cable (wires 4,5,7,8) with the signal pair (wires 1,2,3,6). Power on the spare pair is enabled when the switch port and end device mutually identify themselves as Cisco UPOE-capable using CDP or LLDP and the end device requests for power to be enabled on the spare pair. When the spare pair is powered, the end device can negotiate up to 60 W of power from the switch using CDP or LLDP. Use the **power inline four-pair forced** command when the end device is PoE-capable on both signal and spare pairs, but does not support the CDP or LLDP extensions required for Cisco UPOE.

Use the **max** *max-wattage* option to disallow higher-power powered devices. With this configuration, when the powered device sends Cisco Discovery Protocol (CDP) messages requesting more power than the maximum wattage, the switch removes power from the port. If the powered-device IEEE class maximum is greater than the maximum wattage, the switch does not power the device. The power is reclaimed into the global power budget.

Note The switch never powers any class 0 or class 3 device if the **power inline max max-wattage** command is configured for less than 30 W.

If the switch denies power to a powered device (the powered device requests more power through CDP messages or if the IEEE class maximum is greater than the maximum wattage), the PoE port is in a power-deny

state. The switch generates a system message, and the Oper column in the **show power inline** privileged EXEC command output shows *power-deny*.

Use the **power inline static max** *max-wattage* command to give a port high priority. The switch allocates PoE to a port configured in static mode before allocating power to a port configured in auto mode. The switch reserves power for the static port when it is configured rather than upon device discovery. The switch reserves the power on a static port even when there is no connected device and whether or not the port is in a shutdown or in a no shutdown state. The switch allocates the configured maximum wattage to the port, and the amount is never adjusted through the IEEE class or by CDP messages from the powered device. Because power is pre-allocated, any powered device that uses less than or equal to the maximum wattage is guaranteed power when it is connected to a static port. However, if the powered device IEEE class is greater than the maximum wattage, the switch does not supply power to it. If the switch learns through CDP messages that the powered device needs more than the maximum wattage, the powered device is shut down.

If the switch cannot pre-allocate power when a port is in static mode (for example, because the entire power budget is already allocated to other auto or static ports), this message appears: Command rejected: power inline static: pwr not available. The port configuration remains unchanged.

When you configure a port by using the **power inline auto** or the **power inline static** interface configuration command, the port autonegotiates by using the configured speed and duplex settings. This is necessary to determine the power requirements of the connected device (whether or not it is a powered device). After the power requirements have been determined, the switch hardcodes the interface by using the configured speed and duplex settings without resetting the interface.

When you configure a port by using the **power inline never** command, the port reverts to the configured speed and duplex settings.

If a port has a Cisco powered device connected to it, you should not use the **power inline never** command to configure the port. A false link-up can occur, placing the port in an error-disabled state.

Use the **power inline port priority {high | low}** command to configure the power priority of a PoE port. Powered devices connected to ports with low port priority are shut down first in case of a power shortage.

You can verify your settings by entering the **show power inline** EXEC command.

This example shows how to enable detection of a powered device and to automatically power a PoE port on a switch:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto
```

This example shows how to automatically enable power on both signal and spare pairs from switch port Gigabit Ethernet 1/0/1:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline four-pair forced
```

This example shows how to configure a PoE port on a switch to allow a class 1 or a class 2 powered device:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port on a switch:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline never
```

This example shows how to set the priority of a port to high, so that it would be one of the last ports to be shut down in case of power supply failure:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline port priority high
```

power inline police

To enable policing of real-time power consumption on a powered device, use the **power inline police** command in interface configuration mode. To disable this feature, use the **no** form of this command

power inline police [**action** {**errdisable**| **log**}]

no power inline police

Syntax Description

action errdisable	(Optional) Configures the device to turn off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. This is the default action.
action log	(Optional) Configures the device to generate a syslog message while still providing power to a connected device if the real-time power consumption exceeds the maximum power allocation on the port.

Command Default

Policing of the real-time power consumption of the powered device is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is supported only on the LAN Base image.

This command is supported only on Power over Ethernet (PoE)-capable ports. If you enter this command on a device or port that does not support PoE, an error message appears.

In a switch stack, this command is supported on all switches or ports in the stack that support PoE and real-time power-consumption monitoring.

When policing of the real-time power consumption is enabled, the device takes action when a powered device consumes more power than the allocated maximum amount.

When PoE is enabled, the device senses the real-time power consumption of the powered device. This feature is called *power monitoring* or *power sensing*. The device also polices the power usage with the *power policing* feature.

When power policing is enabled, the device uses one of the these values as the cutoff power on the PoE port in this order:

1. The user-defined power level that limits the power allowed on the port when you enter the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
2. The device automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLPD power negotiation.

If you do not manually configure the cutoff-power value, the device automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the device does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP negotiation, the device might be in violation of the maximum current *Imax* limitation and might experience an *Icut* fault for drawing more current than the maximum. The port remains in the fault state for a time before attempting to power on again. If the port continuously draws more than 15.4 W, the cycle repeats.

When a powered device connected to a PoE+ port restarts and sends a CDP or LLDP packet with a power TLV, the device locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

If power policing is enabled, the device polices power usage by comparing the real-time power consumption to the maximum power allocated on the PoE port. If the device uses more than the maximum power allocation (or *cutoff power*) on the port, the device either turns power off to the port, or the device generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the device to turn off power to the port and put the port in the error-disabled state, use the **power inline police** interface configuration command.
- To configure the device to generate a syslog message while still providing power to the device, use the **power inline police action log** command.

If you do not enter the **action log** keywords, the default action is to shut down the port, turn off power to it, and put the port in the PoE error-disabled state. To configure the PoE port to automatically recover from the error-disabled state, use the **errdisable detect cause inline-power** global configuration command to enable error-disabled detection for the PoE cause and the **errdisable recovery cause inline-power interval** *interval* global configuration command to enable the recovery timer for the PoE error-disabled cause.

Caution If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the port, which could adversely affect the device.

You can verify your settings by entering the **show power inline police** privileged EXEC command.

This example shows how to enable policing of the power consumption and configuring the device to generate a syslog message on the PoE port on a device:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline police action log
```

power supply

To configure and manage the internal power supplies on a switch, use the **power supply** command in privileged EXEC mode.

power supply *stack-member-number* **slot** {**A**| **B**} {**off**| **on**}

Syntax Description

stack-member-number	Stack member number for which to configure the internal power supplies. The range is 1 to 9, depending on the number of switches in the stack. This parameter is available only on stacking-capable switches.
slot	Selects the switch power supply to set.
A	Selects the power supply in slot A.
B	Selects the power supply in slot B. **Note** Power supply slot B is the closest slot to the outer edge of the switch.
off	Sets the switch power supply to off.
on	Sets the switch power supply to on.

Command Default

The switch power supply is on.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **slot** keyword replaced the **frufep** keyword.

Usage Guidelines

The **power supply** command applies to a switch or to a switch stack where all switches are the same platform.

In a switch stack with the same platform switches, you must specify the stack member before entering the **slot** {**A** | **B**} **off** or **on** keywords.

To return to the default setting, use the **power supply** *stack-member-number* **on** command.

You can verify your settings by entering the **show env power** privileged EXEC command.

This example shows how to set the power supply in slot A to off:

```
Device> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

This example shows how to set the power supply in slot A to on:

```
Device> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

This example shows the output of the show env power command:

```
Device> show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  PWR-1RUC2-640WAC    DCB1705B05B OK               Good     Good     250/390
1B  Not Present
```

show CAPWAP summary

To display all the CAPWAP tunnels established by the controller to access points and other mobility controllers use the **show CAPWAP summary** command.

show CAPWAP summary

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CAPWAP tunnels established by the controllers to the access points and other controllers.

```
Device# show capwap summary
CAPWAP Tunnels General Statistics:
Number of Capwap Data Tunnels = 8
Number of Capwap Mobility Tunnels = 0
Number of Capwap Multicast Tunnels = 0
Name APName Type PhyPortIf Mode McastIf
------ ------------------------------- ---- --------- ---------
-------
Ca4 AP-Behind-Router data - unicast -
Ca0 AP1142-kat data - unicast -
Ca5 APRFCHAMBER2-EDISON data - unicast -
Ca6 KATANA_2_RF data - unicast -
```

```
Ca1 AP-1040-RF data - unicast -
Ca7 KATANA_1_RF data - unicast -
Ca2 AP3500-2027 data - unicast -
Ca3 AP-1040-out data - unicast -
```

show controllers cpu-interface

To display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU, use the **show controllers cpu-interface** command in privileged EXEC mode.

show controllers cpu-interface [**switch** *stack-member-number*]

Syntax Description

switch *stack-member-number*	(Optional) Specifies the stack member number.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

This is a partial output example from the **show controllers cpu-interface** command:

```
Device# show controllers cpu-interface switch 1
cpu-queue-frames  retrieved dropped invalid hol-block

----------------  --------- ------- ------- ---------

Routing Protocol          0         0     0     0
L2 Protocol          241567         0     0     0
sw forwarding             0         0     0     0
broadcast             68355         0     0     0
icmp                      0         0     0     0
icmp redirect             0         0     0     0
logging                   0         0     0     0
rpf-fail                  0         0     0     0
DOT1X authentication 328174         0     0     0
Forus Traffic             0         0     0     0
Forus Resolution          0         0     0     0
Wireless q5               0         0     0     0
Wireless q1               0         0     0     0
Wireless q2               0         0     0     0
Wireless q3               0         0     0     0
Wireless q4               0         0     0     0
Learning cache            0         0     0     0
Topology control     820408         0     0     0
Proto snooping            0         0     0     0
```

```
BFD Low latency          0         0     0     0
Transit Traffic          0         0     0     0
Multi End station        0         0     0     0
Health Check             0         0     0     0
Crypto control           0         0     0     0
Exception                0         0     0     0
General Punt             0         0     0     0
NFL sampled data         0         0     0     0
STG cache                0         0     0     0
EGR exception            0         0     0     0
show forward             0         0     0     0
Multicast data           0         0     0     0
Gold packet              0         0     0     0
```

show controllers ethernet-controller

To display per-interface send and receive statistics read from the hardware with keywords, use the **show controllers ethernet-controller** command in EXEC mode.

show controllers ethernet-controller [*interface-id*] [**down-when-looped**| **phy** [**detail**]] [**port-asic statistics** {**exceptions**| **interface** *interface-id* {**l2**| **l3**}| **l3-ifid** *if-id*| **port-ifid** *if-id*| **vlan-ifid** *if-id*} [**switch** *stack-member-number*] [**asic** *asic-number*]]

Syntax Description

interface-id	(Optional) ID of the physical interface.
down-when-looped	(Optional) Displays states related to down-when-looped detection.
phy	(Optional) Displays the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (auto-MDIX) feature on an interface.
detail	(Optional) Displays details about the PHY internal registers.
port-asic	(Optional) Displays information about the port ASIC internal registers.
statistics	Displays port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics.
exceptions	Displays port ASIC exception statistics.
interface *interface-id*	Specifies the interface for which to display port ASIC statistics.
l2	Displays statistics for the Layer 2 interface.
l3	Displays statistics for the Layer 3 interface.
l3-ifid *if-id*	Specifies the Layer 3 IF interface ID for which to display port ASIC statistics.
port-ifid *if-id*	Specifies the PortIF interface ID for which to display port ASIC statistics.
vlan-ifid *if-id*	Specifies the VLANIF interface ID for which to display port ASIC statistics.

switch *stack-member-number*	(Optional) Specifies the stack member number for which to display send and receive statistics.
asic *asic-number*	(Optional) Specifies the ASIC number.

Command Modes

User EXEC (only supported with the *interface-id* keywords in user EXEC mode)

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Without keywords, this command provides the RMON statistics for all interfaces or for the specified interface.

To display the interface internal registers, use the **phy** keyword. To display information about the port ASIC, use the **port-asic** keyword.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

This is an example of output from the **show controllers ethernet-controller** command for an interface:

```
Device# show controllers ethernet-controller gigabitethernet1/0/1
Transmit                 GigabitEthernet1/0/1          Receive
   19216827 Total bytes                            0 Total bytes
      41935 Unicast frames                         0 Unicast frames
    2683840 Unicast bytes                          0 Unicast bytes
     216662 Multicast frames                       0 Multicast frames
   16532987 Multicast bytes                        0 Multicast bytes
          0 Broadcast frames                       0 Broadcast frames
          0 Broadcast bytes                        0 Broadcast bytes
          0 System FCS error frames                0 IpgViolation frames
          0 MacUnderrun frames                     0 MacOverrun frames
          0 Pause frames                           0 Pause frames
          0 Cos 0 Pause frames                     0 Cos 0 Pause frames
          0 Cos 1 Pause frames                     0 Cos 1 Pause frames
          0 Cos 2 Pause frames                     0 Cos 2 Pause frames
          0 Cos 3 Pause frames                     0 Cos 3 Pause frames
          0 Cos 4 Pause frames                     0 Cos 4 Pause frames
          0 Cos 5 Pause frames                     0 Cos 5 Pause frames
          0 Cos 6 Pause frames                     0 Cos 6 Pause frames
          0 Cos 7 Pause frames                     0 Cos 7 Pause frames
          0 Oam frames                             0 OamProcessed frames
          0 Oam frames                             0 OamDropped frames
     251598 Minimum size frames                    0 Minimum size frames
          0 65 to 127 byte frames                  0 65 to 127 byte frames
          0 128 to 255 byte frames                 0 128 to 255 byte frames
       6999 256 to 511 byte frames                 0 256 to 511 byte frames
          0 512 to 1023 byte frames                0 512 to 1023 byte frames
          0 1024 to 1518 byte frames               0 1024 to 1518 byte frames
          0 1519 to 2047 byte frames               0 1519 to 2047 byte frames
          0 2048 to 4095 byte frames               0 2048 to 4095 byte frames
          0 4096 to 8191 byte frames               0 4096 to 8191 byte frames
          0 8192 to 16383 byte frames              0 8192 to 16383 byte frames
          0 16384 to 32767 byte frame              0 16384 to 32767 byte frame
          0 > 32768 byte frames                    0 > 32768 byte frames
          0 Late collision frames                  0 SymbolErr frames
```

```
          0 Excess Defer frames                    0 Collision fragments
          0 Good (1 coll) frames                   0 ValidUnderSize frames
          0 Good (>1 coll) frames                  0 InvalidOverSize frames
          0 Deferred frames                        0 ValidOverSize frames
          0 Gold frames dropped                    0 FcsErr frames
          0 Gold frames truncated
          0 Gold frames successful
          0 1 collision frames
          0 2 collision frames
          0 3 collision frames
          0 4 collision frames
          0 5 collision frames
          0 6 collision frames
          0 7 collision frames
          0 8 collision frames
          0 9 collision frames
          0 10 collision frames
          0 11 collision frames
          0 12 collision frames
          0 13 collision frames
          0 14 collision frames
          0 15 collision frames
          0 Excess collision frames

LAST UPDATE 850 msecs AGO
```

Table 11: Transmit Field Descriptions

Field	Description
Total bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Unicast bytes	The total number of bytes sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Multicast bytes	The total number of bytes sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Broadcast bytes	The total number of bytes sent to broadcast addresses.
System FCS error frames	The total number of frames that fail the Frame Check Sequence (FCS).
MacUnderrun frames	The total number of frames that have MAC Underrun errors.
Pause frames	The total number of pause frames sent on an interface.
Cos x Pause frames	The total number of class of service (CoS) x pause frames sent on an interface.
Oam frames	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames sent on an interface.
Minimum size frames	The number of frames that are the minimum allowed frame size.

Field	Description
65 to 127 byte frames	The total number of frames sent on an interface that are 65 to 127 bytes.
128 to 255 byte frames	The total number of frames sent on an interface that are 128 to 255 bytes.
256 to 511 byte frames	The total number of frames sent on an interface that are 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames sent on an interface that are 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames sent on an interface that are 1024 to 1518 bytes.
1519 to 2047 byte frames	The total number of frames sent on an interface that are 1519 to 2047 bytes.
2048 to 4095 byte frames	The total number of frames sent on an interface that are 2048 to 4095 bytes.
4096 to 8191 byte frames	The total number of frames sent on an interface that are 4096 to 8191 bytes.
8192 to 16383 byte frames	The total number of frames sent on an interface that are 8192 to 16383 bytes.
16384 to 32767 byte frames	The total number of frames sent on an interface that are 16384 to 32767 bytes.
> 32768 byte frames	The total number of frames sent on an interface that are greater than 32768 bytes.
Late collision frames	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.
Good (>1 coll) frames	The number of frames that are successfully sent on an interface after more than one collision occurs. This value does not include the number of frames that are not successfully sent after more than one collision occurs.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
Gold frames dropped	The number of gold frames that are dropped.
Gold frames truncated	The number of gold frames that are truncated.
Gold frames successful	The number of gold frames that are successful.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.

Field	Description
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excess collisions	The number of frames that could not be sent on an interface after 16 collisions occur.

Table 12: Transmit Field Descriptions

Field	Description
Bytes	The total number of bytes sent on an interface.
Unicast Frames	The total number of frames sent to unicast addresses.
Multicast frames	The total number of frames sent to multicast addresses.
Broadcast frames	The total number of frames sent to broadcast addresses.
Too old frames	The number of frames dropped on the egress port because the packet aged out.
Deferred frames	The number of frames that are not sent after the time exceeds 2*maximum-packet time.
MTU exceeded frames	The number of frames that are larger than the maximum allowed frame size.
1 collision frames	The number of frames that are successfully sent on an interface after one collision occurs.
2 collision frames	The number of frames that are successfully sent on an interface after two collisions occur.
3 collision frames	The number of frames that are successfully sent on an interface after three collisions occur.
4 collision frames	The number of frames that are successfully sent on an interface after four collisions occur.
5 collision frames	The number of frames that are successfully sent on an interface after five collisions occur.
6 collision frames	The number of frames that are successfully sent on an interface after six collisions occur.
7 collision frames	The number of frames that are successfully sent on an interface after seven collisions occur.
8 collision frames	The number of frames that are successfully sent on an interface after eight collisions occur.
9 collision frames	The number of frames that are successfully sent on an interface after nine collisions occur.

Field	Description
10 collision frames	The number of frames that are successfully sent on an interface after ten collisions occur.
11 collision frames	The number of frames that are successfully sent on an interface after 11 collisions occur.
12 collision frames	The number of frames that are successfully sent on an interface after 12 collisions occur.
13 collision frames	The number of frames that are successfully sent on an interface after 13 collisions occur.
14 collision frames	The number of frames that are successfully sent on an interface after 14 collisions occur.
15 collision frames	The number of frames that are successfully sent on an interface after 15 collisions occur.
Excessive collisions	The number of frames that could not be sent on an interface after 16 collisions occur.
Late collisions	After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent.
VLAN discard frames	The number of frames dropped on an interface because the CFI[1] bit is set.
Excess defer frames	The number of frames that are not sent after the time exceeds the maximum-packet time.
64 byte frames	The total number of frames sent on an interface that are 64 bytes.
127 byte frames	The total number of frames sent on an interface that are from 65 to 127 bytes.
255 byte frames	The total number of frames sent on an interface that are from 128 to 255 bytes.
511 byte frames	The total number of frames sent on an interface that are from 256 to 511 bytes.
1023 byte frames	The total number of frames sent on an interface that are from 512 to 1023 bytes.
1518 byte frames	The total number of frames sent on an interface that are from 1024 to 1518 bytes.

Field	Description
Too large frames	The number of frames sent on an interface that are larger than the maximum allowed frame size.
Good (1 coll) frames	The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs.

[1] CFI = Canonical Format Indicator

Table 13: Receive Field Descriptions

Field	Description
Total Bytes	The total amount of memory (in bytes) used by frames received on an interface, including the FCS[2] value and the incorrectly formed frames. This value excludes the frame header bits.
Unicast frames	The total number of frames successfully received on the interface that are directed to unicast addresses.
Unicast bytes	The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast frames	The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
Multicast bytes	The total number of bytes successfully received on the interface that are directed to multicast addresses.
Broadcast frames	The total number of frames successfully received on an interface that are directed to broadcast addresses.
Broadcast bytes	The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits.
IpgViolation frames	The total number of frames with an interpacket gap (IPG) violation.
MacOverrun frames	The total number of frames with MacOverrun errors.
Pause frames	The total number of pause frames received on an interface.
Cos x Pause frames	The total number of class of service (CoS) x pause frames received on an interface.

Field	Description
OamProcessed	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames that are processed on an interface.
OamDropped	The total number of Ethernet Operations, Administration, and Maintenance (OAM) frames that are dropped on an interface.
Minimum size frames	The total number of frames that are the minimum frame size.
65 to 127 byte frames	The total number of frames that are from 65 to 127 bytes.
128 to 255 byte frames	The total number of frames that are from 128 to 255 bytes.
256 to 511 byte frames	The total number of frames that are from 256 to 511 bytes.
512 to 1023 byte frames	The total number of frames that are from 512 to 1023 bytes.
1024 to 1518 byte frames	The total number of frames that are from 1024 to 1518 bytes.
1519 to 2047 byte frames	The total number of frames that are from 1519 to 2047 bytes.
2048 to 4095 byte frames	The total number of frames that are from 2048 to 4095 bytes.
4096 to 8191 byte frames	The total number of frames that are from 4096 to 8191 bytes.
8192 to 16383 byte frames	The total number of frames that are from 8192 to 16383 bytes.
16384 to 32767 byte frames	The total number of frames that are from 16384 to 32767 bytes.
> 32768 byte frames	The total number of frames that are greater than 32768 bytes.
Symbol error frames	The number of frames received on an interface that have symbol errors.
Collision fragments	The number of collision fragments received on an interface.
Valid undersize frames	The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits.
Invalid oversize frames	The number of frames received that were larger than maximum allowed maximum transmission unit (MTU) size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error.
Valid oversize frames	The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag.

Field	Description
FcsErr frames	The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values.

2 FCS = frame check sequence

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface:

```
Device# show controllers ethernet-controller gigabitethernet1/0/2 phy
Gi1/0/2 (gpn: 2, port-number: 2)
------------------------------------------------------------
 0000 : 1140  Control Register                  :  0001 0001 0100 0000
 0001 : 7949  Control STATUS                    :  0111 1001 0100 1001
 0002 : 0141  Phy ID 1                          :  0000 0001 0100 0001
 0003 : 0EE0  Phy ID 2                          :  0000 1110 1110 0000
 0004 : 03E1  Auto-Negotiation Advertisement    :  0000 0011 1110 0001
 0005 : 0000  Auto-Negotiation Link Partner     :  0000 0000 0000 0000
 0006 : 0004  Auto-Negotiation Expansion Reg    :  0000 0000 0000 0100
 0007 : 2001  Next Page Transmit Register       :  0010 0000 0000 0001
 0008 : 0000  Link Partner Next page Registe    :  0000 0000 0000 0000
 0010 : 3B60  PHY Specific Control              :  0011 1011 0110 0000
 0011 : 8010  PHY Specific Status               :  1000 0000 0001 0000
 0012 : 6404  PHY Specific Interrupt Enable     :  0110 0100 0000 0100
 0013 : 0000  PHY Specific Interrupt Status     :  0000 0000 0000 0000
```

show controllers utilization

To display bandwidth utilization, use the **show controllers utilization** command in EXEC mode.

show controllers [*interface-id*] **utilization**

Syntax Description

interface-id	(Optional) ID of the physical interface.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show controllers utilization** command:

```
Device> show controllers utilization
Port       Receive Utilization  Transmit Utilization
```

```
Gi1/0/1            0                    0
Gi1/0/2            0                    0
Gi1/0/3            0                    0
Gi1/0/4            0                    0
Gi1/0/5            0                    0
Gi1/0/6            0                    0
Gi1/0/7            0                    0
<output truncated>
Gi2/0/1            0                    0
Gi2/0/2            0                    0
<output truncated>
Total Ports : 48
Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Average Switch Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Device> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

Table 14: Show controllers utilization Field Descriptions

Field	Description
Receive Bandwidth Percentage Utilization	Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity.
Transmit Bandwidth Percentage Utilization	Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity.
Average Switch Percentage Utilization	Displays the average of the transmitted and received bandwidth usage of the switch.

show eee

To display Energy Efficient Ethernet (EEE) information for an interface, use the **show eee** command in EXEC mode.

show eee {**capabilities**| **status**} **interface** *interface-id*

Syntax Description

capabilities	Displays EEE capabilities for the specified interface.
status	Displays EEE status information for the specified interface.
interface *interface-id*	Specifies the interface for which to display EEE capabilities or status information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low power utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

To check if an interface is EEE capable, use the **show eee capabilities** command. You can enable EEE on an interface that is EEE capable by using the **power efficient-ethernet auto** interface configuration command.

To view the EEE status, LPI status, and wake error count information for an interface, use the **show eee status** command.

This is an example of output from the **show eee capabilities** command on an interface where EEE is enabled:

```
Device# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
        EEE(efficient-ethernet):  yes (100-Tx and 1000T auto)
        Link Partner           :  yes (100-Tx and 1000T auto)
```

This is an example of output from the **show eee capabilities** command on an interface where EEE is not enabled:

```
Device# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
        EEE(efficient-ethernet):  not enabled
        Link Partner           :  not enabled
```

This is an example of output from the **show eee status** command on an interface where EEE is enabled and operational. The table that follows describes the fields in the display.

```
Device# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
        EEE(efficient-ethernet):  Operational
        Rx LPI Status          :  Received
        Tx LPI Status          :  Received
```

This is an example of output from the **show eee status** command on an interface where EEE operational and the ports are in low power save mode:

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
        EEE(efficient-ethernet):  Operational
```

```
        Rx LPI Status          :  Low Power
        Tx LPI Status          :  Low Power
        Wake Error Count       :  0
```

This is an example of output from the **show eee status** command on an interface where EEE is not enabled because a remote link partner is incompatible with EEE:

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
        EEE(efficient-ethernet):  Disagreed
        Rx LPI Status          :  None
        Tx LPI Status          :  None
        Wake Error Count       :  0
```

Table 15: show eee status Field Descriptions

Field	Description
EEE (efficient-ethernet)	The EEE status for the interface. This field can have any of the following values: • N/A—The port is not capable of EEE. • Disabled—The port EEE is disabled. • Disagreed—The port EEE is not set because a remote link partner might be incompatible with EEE; either it is not EEE capable, or its EEE setting is incompatible. • Operational—The port EEE is enabled and operating. If the interface speed is configured as 10 Mbps, EEE is disabled internally. When the interface speed moves back to auto, 100 Mbps or 1000 Mbps, EEE becomes active again.

Field	Description
Rx/Tx LPI Status	The Low Power Idle (LPI) status for the link partner. These fields can have any of the following values: • N/A—The port is not capable of EEE. • Interrupted—The link partner is in the process of moving to low power mode. • Low Power—The link partner is in low power mode. • None— EEE is disabled or not capable at the link partner side. • Received—The link partner is in low power mode and there is traffic activity. If an interface is configured as half-duplex, the LPI status is None, which means the interface cannot be in low power mode until it is configured as full-duplex.
Wake Error Count	The number of PHY wake-up faults that have occurred. A wake-up fault can occur when EEE is enabled and the connection to the link partner is broken. This information is useful for PHY debugging.

show env

To display fan, temperature, and power information, use the **show env** command in EXEC mode.

show env {**all**| **fan**| **power** [**all**| **switch** [*stack-member-number*]]| **stack** [*stack-member-number*] | **temperature** [**status**]}

Syntax Description

all	Displays the fan and temperature environmental status and the status of the internal power supplies.
fan	Displays the switch fan status.
power	Displays the internal power status of the active switch.
all	(Optional) Displays the status of all the internal power supplies in a standalone switch when the command is entered on the switch, or in all the stack members when the command is entered on the active switch.

switch	(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
stack-member-number	(Optional) Number of the stack member for which to display the status of the internal power supplies or the environmental status. The range is 1 to 9.
stack	Displays all environmental status for each switch in the stack or for the specified switch. This keyword is available only on stacking-capable switches.
temperature	Displays the switch temperature status.
status	(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show env** EXEC command to display the information for the switch being accessed—a standalone switch or the active switch. Use this command with the **stack** and **switch** keywords to display all information for the stack or for the specified stack member.

If you enter the **show env temperature status** command, the command output shows the switch temperature state and the threshold level.

You can also use the **show env temperature** command to display the switch temperature status. The command output shows the green and yellow states as *OK* and the red state as *FAULTY*. If you enter the **show env all** command, the command output is the same as the **show env temperature status** command output.

This is an example of output from the **show env all** command:

```
Device>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
```

```
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

This is an example of output from the **show env fan** command:

```
Device>show env fan
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
```

This is an example of output from the **show env power** command:

```
Device>show env power
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

This is an example of output from the **show env power all** command on the active switch:

```
Device# show env power all
SW  PID                 Serial#     Status           Sys Pwr  PoE Pwr  Watts
--  ------------------  ----------  ---------------  -------  -------  -----
1A  Not Present
1B  PWR-C1-715WAC       LIT150119Z1  OK              Good     Good     715
```

This is an example of output from the **show env stack** command on the active switch:

```
Device> show env stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 28 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
```

This example shows how to display the temperature value, state, and the threshold values on a standalone switch. The table describes the temperature states in the command output.

```
Device> show env temperature status
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
```

Table 16: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.

State	Description
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show errdisable detect

To display error-disabled detection status, use the **show errdisable detect** command in EXEC mode.

show errdisable detect

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A gbic-invalid error reason refers to an invalid small form-factor pluggable (SFP) module.

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error-disable is configured for each feature.

You can configure error-disabled detection in these modes:

- port mode—The entire physical port is error-disabled if a violation occurs.
- vlan mode—The VLAN is error-disabled if a violation occurs.
- port/vlan mode—The entire physical port is error-disabled on some ports and is per-VLAN error-disabled on other ports.

This is an example of output from the **show errdisable detect** command:

```
Device> show errdisable detect
ErrDisable Reason    Detection    Mode
-----------------    ---------    ----
arp-inspection       Enabled      port
bpduguard            Enabled      vlan
channel-misconfig    Enabled      port
community-limit      Enabled      port
```

```
dhcp-rate-limit      Enabled      port
dtp-flap             Enabled      port
gbic-invalid         Enabled      port
inline-power         Enabled      port
invalid-policy       Enabled      port
l2ptguard            Enabled      port
link-flap            Enabled      port
loopback             Enabled      port
lsgroup              Enabled      port
pagp-flap            Enabled      port
psecure-violation    Enabled      port/vlan
security-violatio    Enabled      port
sfp-config-mismat    Enabled      port
storm-control        Enabled      port
udld                 Enabled      port
vmps                 Enabled      port
```

show errdisable recovery

To display the error-disabled recovery timer information, use the **show errdisable recovery** command in EXEC mode.

show errdisable recovery

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.

Note Though visible in the output, the unicast-flood field is not valid.

This is an example of output from the **show errdisable recovery** command:

```
Device> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
```

```
vmps                Disabled
pagp-flap           Disabled
dtp-flap            Disabled
link-flap           Enabled
l2ptguard           Disabled
psecure-violation   Disabled
gbic-invalid        Disabled
dhcp-rate-limit     Disabled
unicast-flood       Disabled
storm-control       Disabled
arp-inspection      Disabled
loopback            Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi1/0/2        link-flap             279
```

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*interface-id*| **vlan** *vlan-id*] [**accounting**| **capabilities** [**module** *number*]| **debounce**| **description**| **etherchannel**| **flowcontrol**| **pruning**| **stats**| **status** [**err-disabled**| **inactive**]| **trunk**]

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
vlan *vlan-id*	(Optional) VLAN identification. The range is 1 to 4094.
accounting	(Optional) Displays accounting information on the interface, including active protocols and input and output packets and octets. **Note** The display shows only packets processed in software; hardware-switched packets do not appear.
capabilities	(Optional) Displays the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs.
module *number*	(Optional) Displays capabilities of all interfaces on the switch or specified stack member. The range is 1 to 9. This option is not available if you entered a specific interface ID.
debounce	(Optional) Displays port debounce timer information for an interface.

description	(Optional) Displays the administrative status and description set for an interface.
etherchannel	(Optional) Displays interface EtherChannel information.
flowcontrol	(Optional) Displays interface flow control information.
mtu	(Optional) Displays the MTU for each interface or for the specified interface.
pruning	(Optional) Displays trunk VTP pruning information for the interface.
stats	(Optional) Displays the input and output packets by switching the path for the interface.
status	(Optional) Displays the status of the interface. A status of unsupported in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot.
err-disabled	(Optional) Displays interfaces in an error-disabled state.
inactive	(Optional) Displays interfaces in an inactive state.
trunk	(Optional) Displays interface trunk information. If you do not specify an interface, only information for active trunking ports appears.

Note Though visible in the command-line help strings, the **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **random-detect**, and **rate-limit** keywords are not supported.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module** *number* command to display the capabilities of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces in the stack.

This is an example of output from the **show interfaces** command for an interface on stack member 3:

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command:

This is an example of output from the **show interfaces capabilities** command for an interface:

```
Device# show interfaces gigabitethernet1/0/2 capabilities
GigabitEthernet1/0/2
  Model:                 UA-3850-24-CR
  Type:                  10/100/1000BaseTX
  Speed:                 10,100,1000,auto
  Duplex:                full,half,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),
                         tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
  Inline power:          no
  SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

```
Device# show interfaces gigabitethernet1/0/2 description
Interface                      Status         Protocol Description
```

```
Gi1/0/2                        up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Device# show interfaces etherchannel
----
Port-channel34:
Age of the Port-channel   = 28d:18h:51m:46s
Logical slot/port   = 12/34          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Passive port list   =
Port state          = Port-channel L3-Ag Ag-Not-Inuse
Protocol            =    -
Port security       = Disabled
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command when pruning is enabled in the VTP domain:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```
Device# show interfaces vlan 1 stats
Switching path    Pkts In    Chars In    Pkts Out    Chars Out
     Processor    1165354   136205310      570800     91731594
   Route cache          0           0           0            0
         Total    1165354   136205310      570800     91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces:

This is an example of output from the **show interfaces** *interface-id* **status** command:

```
Device# show interfaces gigabitethernet1/0/20 status
Port      Name               Status       Vlan       Duplex  Speed       Type
Gi1/0/20                     notconnect   1            auto   auto 10/100/1000Ba
seTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Device# show interfaces status err-disabled
Port      Name       Status         Reason
Gi1/0/2              err-disabled   gbic-invalid
Gi2/0/3              err-disabled   dtp-flap
```

This is an example of output from the **show interfaces** *interface-id* **pruning** command:

```
Device# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

This is an example of output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port        Mode             Encapsulation  Status        Native vlan
Gi1/0/1     on               802.1q         other         10

Port        Vlans allowed on trunk
Gi1/0/1     none

Port        Vlans allowed and active in management domain
Gi1/0/1     none
```

```
Port        Vlans in spanning tree forwarding state and not pruned
Gi1/0/1     none
```

show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

show interfaces [*interface-id*] **counters** [**errors**| **etherchannel**| **module** *stack-member-number*| **protocol status**| **trunk**]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
errors	(Optional) Displays error counters.
etherchannel	(Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
module *stack-member-number*	(Optional) Displays counters for the specified stack member. The range is 1 to 9. **Note** In this command, the **module** keyword refers to the stack member number. The module number that is part of the interface ID is always zero.
protocol status	(Optional) Displays the status of protocols enabled on interfaces.
trunk	(Optional) Displays trunk counters.

Note Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Device# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1               0              0              0              0
Gi1/0/2               0              0              0              0
Gi1/0/3        95285341          43115        1178430           1950
Gi1/0/4               0              0              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Device# show interfaces counters module 2
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Gi1/0/1             520              2              0              0
Gi1/0/2             520              2              0              0
Gi1/0/3             520              2              0              0
Gi1/0/4             520              2              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces:

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Device# show interfaces counters trunk
Port        TrunkFramesTx   TrunkFramesRx   WrongEncap
Gi1/0/1                 0               0            0
Gi1/0/2                 0               0            0
Gi1/0/3             80678               0            0
Gi1/0/4             82320               0            0
Gi1/0/5                 0               0            0

<output truncated>
```

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings, use the **show interfaces switchport** command in privileged EXEC mode.

show interfaces [*interface-id*] **switchport** [**module** *number*]

Syntax Description

interface-id	(Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.
module *number*	(Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. The range is 1 to 9. This option is not available if you entered a specific interface ID.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show interface switchport module** *number* command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

This is an example of output from the **show interfaces switchport** command for a port. The table that follows describes the fields in the display.

Note Private VLANs are not supported in this release, so those fields are not applicable.

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
```

```
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.

Field	Description
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

show interfaces transceiver

To display the physical properties of a small form-factor pluggable (SFP) module interface, use the **show interfaces transceiver** command in EXEC mode.

show interfaces [*interface-id*] **transceiver** [**detail**| **module** *number*| **properties**| **supported-list**| **threshold-table**]

Syntax Description

interface-id	(Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
detail	(Optional) Displays calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
module *number*	(Optional) Limits display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
properties	(Optional) Displays speed, duplex, and inline power settings on an interface.
supported-list	(Optional) Lists all supported transceivers.
threshold-table	(Optional) Displays alarm and warning threshold table.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show interfaces** *interface-id* **transceiver properties** command:

```
Device# show interfaces gigabitethernet1/1/1 transceiver properties
  Name : Gi1/1/1
  Administrative Speed: auto
```

```
  Operational Speed: auto
  Administrative Duplex: auto
  Administrative Power Inline: enable
  Operational Duplex: auto
  Administrative Auto-MDIX: off
  Operational Auto-MDIX: off
```

This is an example of output from the **show interfaces** *interface-id* **transceiver detail** command:

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
  ITU Channel not available (Wavelength not available),
  Transceiver is internally calibrated.
  mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
  ++:high alarm, +:high warning, -:low warning, -- :low alarm.
  A2D readouts (if they differ), are reported in parentheses.
  The threshold values are uncalibrated.

                            High Alarm  High Warn  Low Warn   Low Alarm
          Temperature       Threshold   Threshold  Threshold  Threshold
  Port    (Celsius)        (Celsius)   (Celsius)  (Celsius)  (Celsius)
  -------  -----------------  ----------  ---------  ---------  ---------
  Gi1/1/1  29.9               74.0        70.0       0.0        -4.0
                            High Alarm  High Warn  Low Warn   Low Alarm
          Voltage           Threshold   Threshold  Threshold  Threshold
  Port    (Volts)           (Volts)     (Volts)    (Volts)    (Volts)
  -------  ---------------    ----------  ---------  ---------  ---------
  Gi1/1/1  3.28               3.60        3.50       3.10       3.00

          Optical           High Alarm  High Warn  Low Warn   Low Alarm
          Transmit Power    Threshold   Threshold  Threshold  Threshold
  Port    (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
  -------  -----------------  ----------  ---------  ---------  ---------
  Gi1/1/1  1.8                7.9         3.9        0.0        -4.0

          Optical           High Alarm  High Warn  Low Warn   Low Alarm
          Receive Power     Threshold   Threshold  Threshold  Threshold
  Port    (dBm)             (dBm)       (dBm)      (dBm)      (dBm)
  -------  -----------------  ----------  ---------  ---------  ---------
  Gi1/1/1  -23.5              -5.0        -9.0       -28.2      -32.2
```

This is an example of output from the **show interfaces transceiver threshold-table** command:

```
Device# show interfaces transceiver threshold-table
              Optical Tx     Optical Rx    Temp     Laser Bias    Voltage
                                                     current
             -------------  -------------  ------   ------------  ---------

 DWDM GBIC
Min1             -4.00        -32.00        -4            N/A          4.65
Min2              0.00        -28.00        0             N/A          4.75
Max2              4.00         -9.00        70            N/A          5.25
Max1              7.00         -5.00        74            N/A          5.40
 DWDM SFP
Min1             -4.00        -32.00        -4            N/A          3.00
Min2              0.00        -28.00        0             N/A          3.10
Max2              4.00         -9.00        70            N/A          3.50
Max1              8.00         -5.00        74            N/A          3.60
 RX only WDM GBIC
Min1              N/A         -32.00        -4            N/A          4.65
Min2              N/A         -28.30        0             N/A          4.75
Max2              N/A          -9.00        70            N/A          5.25
Max1              N/A          -5.00        74            N/A          5.40
 DWDM XENPAK
Min1             -5.00        -28.00        -4            N/A          N/A
Min2             -1.00        -24.00        0             N/A          N/A
Max2              3.00         -7.00        70            N/A          N/A
Max1              7.00         -3.00        74            N/A          N/A
 DWDM X2
Min1             -5.00        -28.00        -4            N/A          N/A
Min2             -1.00        -24.00        0             N/A          N/A
Max2              3.00         -7.00        70            N/A          N/A
```

```
Max1              7.00         -3.00        74            N/A          N/A
 DWDM XFP
Min1             -5.00        -28.00        -4            N/A          N/A
Min2             -1.00        -24.00        0             N/A          N/A
Max2              3.00         -7.00        70            N/A          N/A
Max1              7.00         -3.00        74            N/A          N/A
 CWDM X2
Min1              N/A           N/A         0             N/A          N/A
Min2              N/A           N/A         0             N/A          N/A
Max2              N/A           N/A         0             N/A          N/A
Max1              N/A           N/A         0             N/A          N/A

<output truncated>
```

show memory platform

To display memory statistics of a platform, use the **show memory platform** command in privileged EXEC mode.

show memory platform [**compressed-swap** | **information** | **page-merging**]

Syntax Description

compressed-swap	(Optional) Displays platform memory compressed-swap information.
information	(Optional) Displays general information about the platform.
page-merging	(Optional) Displays platform memory page-merging information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

The following is sample output from the **show memory platform** command:

```
Switch# show memory platform

 Virtual memory   : 12874653696
  Pages resident   : 627041
  Major page faults: 2220
  Minor page faults: 2348631

  Architecture     : mips64
```

```
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761276
    Free           : 1215576
    Active         : 2128196
    Inactive       : 1581856
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 0
    AnonPages      : 1294984
    Bounce         : 0
    Cached         : 1978168
    Commit Limit   : 1988424
    Committed As   : 3343324
    High Total     : 0
    High Free      : 0
    Low Total      : 3976852
    Low Free       : 1215576
    Mapped         : 516316
    NFS Unstable   : 0
    Page Tables    : 17124
    Slab           : 0
    VMmalloc Chunk : 1069542588
    VMmalloc Total : 1069547512
    VMmalloc Used  : 2588
    Writeback      : 0
    HugePages Total: 0
    HugePages Free : 0
    HugePages Rsvd : 0
    HugePage Size  : 2048

  Swap (kB)
    Total          : 0
    Used           : 0
    Free           : 0
    Cached         : 0

  Buffers (kB)     : 437136

  Load Average
    1-Min          : 1.04
    5-Min          : 1.16
    15-Min         : 0.94
```

The following is sample output from the **show memory platform information** command:

```
Device# show memory platform information

 Virtual memory   : 12870438912
  Pages resident   : 626833
  Major page faults: 2222
  Minor page faults: 2362455

  Architecture     : mips64
  Memory (kB)
    Physical       : 3976852
    Total          : 3976852
    Used           : 2761224
    Free           : 1215628
    Active         : 2128060
    Inactive       : 1584444
    Inact-dirty    : 0
    Inact-clean    : 0
    Dirty          : 284
    AnonPages      : 1294656
    Bounce         : 0
    Cached         : 1979644
    Commit Limit   : 1988424
    Committed As   : 3342184
    High Total     : 0
    High Free      : 0
```

```
  Low Total      : 3976852
  Low Free       : 1215628
  Mapped         : 516212
  NFS Unstable   : 0
  Page Tables    : 17096
  Slab           : 0
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 438228

Load Average
  1-Min          : 1.54
  5-Min          : 1.27
  15-Min         : 0.99
```

show module

To display module information such as switch number, model number, serial number, hardware revision number, software version, MAC address and so on, use this command in user EXEC or privileged EXEC mode.

show module [*switch-num*]

Syntax Description

switch-num	(Optional) Number of the switch.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Entering the **show module** command without the *switch-num* argument is the same as entering the show module all command.

This example shows how to display information for all the modules on a Cisco Catalyst 3850 Series switch:

show mgmt-infra trace messages ilpower

To display inline power messages within a trace buffer, use the **show mgmt-infra trace messages ilpower** command in privileged EXEC mode.

show mgmt-infra trace messages ilpower [**switch** *stack-member-number*]

Syntax Description

switch *stack-member-number*	(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an output example from the **show mgmt-infra trace messages ilpower** command:

```
Device# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
```

```
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

show mgmt-infra trace messages ilpower-ha

To display inline power high availability messages within a trace buffer, use the **show mgmt-infra trace messages ilpower-ha** command in privileged EXEC mode.

show mgmt-infra trace messages ilpower-ha [**switch** *stack-member-number*]

Syntax Description

switch *stack-member-number*	(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an output example from the **show mgmt-infra trace messages ilpower-ha** command:

```
Device# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client succ
essfully.
```

show mgmt-infra trace messages platform-mgr-poe

To display platform manager Power over Ethernet (PoE) messages within a trace buffer, use the **show mgmt-infra trace messages platform-mgr-poe** privileged EXEC command.

show mgmt-infra trace messages platform-mgr-poe [**switch** *stack-member-number*]

Syntax Description

switch *stack-member-number*	(Optional) Specifies the stack member number for which to display messages within a trace buffer.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of partial output from the **show mgmt-infra trace messages platform-mgr-poe** command:

```
Device# show mgmt-infra trace messages platform-mgr-poe
[10/23/12 14:04:06.431 UTC 1 5495] PoE Info: get power controller param sent:
[10/23/12 14:04:06.431 UTC 2 5495] PoE Info: POE_SHUT sent for port 1 (0:0)
[10/23/12 14:04:06.431 UTC 3 5495] PoE Info: POE_SHUT sent for port 2 (0:1)
[10/23/12 14:04:06.431 UTC 4 5495] PoE Info: POE_SHUT sent for port 3 (0:2)
[10/23/12 14:04:06.431 UTC 5 5495] PoE Info: POE_SHUT sent for port 4 (0:3)
[10/23/12 14:04:06.431 UTC 6 5495] PoE Info: POE_SHUT sent for port 5 (0:4)
[10/23/12 14:04:06.431 UTC 7 5495] PoE Info: POE_SHUT sent for port 6 (0:5)
[10/23/12 14:04:06.431 UTC 8 5495] PoE Info: POE_SHUT sent for port 7 (0:6)
[10/23/12 14:04:06.431 UTC 9 5495] PoE Info: POE_SHUT sent for port 8 (0:7)
[10/23/12 14:04:06.431 UTC a 5495] PoE Info: POE_SHUT sent for port 9 (0:8)
[10/23/12 14:04:06.431 UTC b 5495] PoE Info: POE_SHUT sent for port 10 (0:9)
[10/23/12 14:04:06.431 UTC c 5495] PoE Info: POE_SHUT sent for port 11 (0:10)
[10/23/12 14:04:06.431 UTC d 5495] PoE Info: POE_SHUT sent for port 12 (0:11)
[10/23/12 14:04:06.431 UTC e 5495] PoE Info: POE_SHUT sent for port 13 (e:0)
[10/23/12 14:04:06.431 UTC f 5495] PoE Info: POE_SHUT sent for port 14 (e:1)
[10/23/12 14:04:06.431 UTC 10 5495] PoE Info: POE_SHUT sent for port 15 (e:2)
[10/23/12 14:04:06.431 UTC 11 5495] PoE Info: POE_SHUT sent for port 16 (e:3)
[10/23/12 14:04:06.431 UTC 12 5495] PoE Info: POE_SHUT sent for port 17 (e:4)
[10/23/12 14:04:06.431 UTC 13 5495] PoE Info: POE_SHUT sent for port 18 (e:5)
[10/23/12 14:04:06.431 UTC 14 5495] PoE Info: POE_SHUT sent for port 19 (e:6)
[10/23/12 14:04:06.431 UTC 15 5495] PoE Info: POE_SHUT sent for port 20 (e:7)
[10/23/12 14:04:06.431 UTC 16 5495] PoE Info: POE_SHUT sent for port 21 (e:8)
[10/23/12 14:04:06.431 UTC 17 5495] PoE Info: POE_SHUT sent for port 22 (e:9)
[10/23/12 14:04:06.431 UTC 18 5495] PoE Info: POE_SHUT sent for port 23 (e:10)
```

show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

show network-policy profile [*profile-number*]

Syntax Description

profile-number	(Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show network-policy profile** command:

```
Device# show network-policy profile
Network Policy Profile 60
  Interface:
   none
```

show platform CAPWAP summary

To display the tunnel identifier and the type all the CAPWAP tunnels established by the controller to the access points and other mobility controllers, use the **show platform CAPWAP summary** command.

show platform CAPWAP summary

Syntax Description This command has no arguments or keywords.

Command Default

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example displays the tunnel identifier and details:

```
Device# show platform capwap summary
Tunnel ID | Type | Src IP | Dst IP | SPrt | DPrt | S | A
--------------------------------------------------------------------------------

0x0088498000000983 data 9.6.44.61 9.12.138.101 5247 41894 1 1

0x00966dc000000010 data 9.6.44.61 9.6.47.101 5247 62526 1 2
0x00938e800000095b data 9.6.44.61 9.12.138.100 5247 45697 1 1

0x00ab1a8000000bd1 data 9.6.44.61 9.12.139.101 5247 38906 1 0
```

```
0x00896e40000000bd data 9.6.44.61 9.12.136.100 5247 1836 1 1
```

show platform forward

Use the **show platform forward** privileged EXEC command for an interface to display how the hardware would forward a frame that matches the specified parameters.

show platform forward *interface-id* [**vlan** *vlan-id*] *src-macdst-mac* [*l3protocol-id*] [**ipv6** | **sap** | **snap**] [**cos** *cos* [**ip** *src-ip dst-ip* [**frag** *field*] [**dscp** *dscp*] { *l4protocol-id* | **icmp** *icmp-type icmp-code* | **igmp** *igmp-version igmp-type* | **sctp** *src-port dst-port* | **tcp** *src-post dst-port flags* | **udp** *src-port dst-port*] } [| { **begin** | **exclude** | **include** } *expression*]

Syntax Description

interface-id	The input physical interface, the port on which the packet comes in to the switch (including type and port number).
vlan *vlan-id*	(Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1.
src-mac	48-bit source MAC address.
dst-mac	48-bit destination MAC address.
ipv6	(Optional) IPv6 frame. This keyword is available only if the switch is running the IP services image.
sap	(Optional) Service access point (SAP) encapsulation type.
snap	(Optional) Subnetwork Access Protocol (SNAP) encapsulation type.
cos *cos*	(Optional) Class of service (CoS) value of the frame. The range is 0 to 7.
ip *src-ip dst-ip*	(Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation.
frag *field*	(Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535.
dscp *dscp*	(Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63.
l4protocol-id	The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), or Internet Group Management Protocol (IGMP), you should use the appropriate keyword instead of a numeric value.
icmp *icmp-type icmp-code*	ICMP parameters. The icmp-type and icmp-code ranges are 0 to 255.

igmp *igmp-version igmp-type*	IGMP parameters. The *igmp-version* range is 1 to 15; the *igmp-type* range is 0 to 15.
sctp *src-port dst-port*	Stream Control Transmission Protocol (SCTP) parameters. The ranges for the SCTP source and destination ports are 0 to 65535.
tcp *src-post dst-port flags*	TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The src-port and dst-port ranges are 0 to 65535. The flag range is 0 to 1024.
udp *src-port dst-port*	UDP parameters. The src-port and dst-port ranges are 0 to 65535.
| begin	(Optional) Display begins with the line that matches the *expression*.
| exclude	(Optional) Display excludes lines that match the *expression*.
| include	(Optional) Display includes lines that match the specified *expression*.
expression	Expression in the output to use as a reference point.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

show platform hardware fed switch forward

To display device-specific hardware information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the forwarding-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** command.

The output of the **show platform hardware fed switch** *switch_number* **forward summary** displays all the details about the forwarding decision taken for the packet.

show platform hardware fed switch {*switch_num*| **active**| **standby**} **forward summary**

Syntax Description

switch {*switch_num* | **active** | **standby** }	The switch for which you want to display information. You have the following options : • *switch_num*—ID of the switch. • **active**—Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available.
forward summary	Displays packet forwarding information.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Do not use this command unless a technical support representative asks you to. Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Fields displayed in the command output are explained below.

- Station Index : The Station Index is the result of the layer 2 lookup and points to a station descriptor which provides the following:
  - Destination Index : Determines the egress port(s) to which the packets should be sent to. Global Port Number(GPN) can be used as the destination index. A destination index with15 down to 12 bits set indicates the GPN to be used. For example, destination index - 0xF04E corresponds to GPN - 78 (0x4e).
  - Rewrite Index : Determines what needs to be done with the packets. For layer 2 switching, this is typically a bridging action
  - Flexible Lookup Pipeline Stages(FPS) : Indicates the forwarding decision that was taken for the packet - routing or bridging
  - Replication Bit Map : Determines if the packets should be sent to CPU or stack
    - Local Data Copy = 1
    - Remote Data copy = 0
    - Local CPU Copy = 0
    - Remote CPU Copy = 0

Example

This is an example of output from the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** command.

```
Device#show platform hardware fed switch 1 forward summary
Time: Fri Sep 16 08:25:00 PDT 2016

Incomming Packet Details:

###[ Ethernet ]###
  dst       = 00:51:0f:f2:0e:11
  src       = 00:1d:01:85:ba:22
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = 6
     plen      = 4
     op        = is-at
     hwsrc     = 00:1d:01:85:ba:22
     psrc      = 10.10.1.33
     hwdst     = 00:51:0f:f2:0e:11
     pdst      = 10.10.1.1

Ingress:
Switch             : 1
Port               : GigabitEthernet1/0/1
Global Port Number : 1
Local Port Number  : 1
Asic Port Number   : 21
ASIC Number        : 0
STP state          :
                    blkLrn31to0: 0xffdfffdf
                    blkFwd31to0: 0xffdfffdf
Vlan               : 1
Station Descriptor : 170
DestIndex          : 0xF009
DestModIndex       : 2
RewriteIndex       : 2
Forwarding Decision: FPS 2A L2 Destination

Replication Bitmap:
Local CPU copy     : 0
Local Data copy    : 1
Remote CPU copy    : 0
Remote Data copy   : 0

Egress:
Switch             : 1
Outgoing Port      : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number        : 0
Vlan               : 1
```

show platform resources

To display platform resource information, use the **show platform reources** command in privileged EXEC mode.

show platform resources

This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The output of this command displays the used memory, which is total memory minus the accurate free memory.

Example

The following is sample output from the **show platform resources** command:

```
Switch# show platform resources

**State Acronym: H - Healthy, W - Warning, C - Critical

Resource                 Usage                 Max             Warning         Critical
     State
-----------------------------------------------------------------------------------------------

 Control Processor       7.20%                 100%            90%             95%
     H
  DRAM                   2701MB(69%)           3883MB          90%             95%
     H
```

show platform software ilpower

To display the inline power details of all the PoE ports on the device, use the **show platform software ilpower** command in privileged EXEC mode.

show platform software ilpower {**details** | **port** {**GigabitEthernet** *interface-number* } | **system** *slot-number* }

Syntax Description

details	Displays inline power details for all the interfaces.
port	Displays inline power port configuration.
GigabitEthernet *interface-number*	The GigabitEthernet interface number. Values range from 0 to 9.
system *slot-number*	Displays inline power system configuration.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was modified. The keyword **details** argument was added.
Cisco IOS XE Denali 16.1.1	The command was introduced.

Example

The following is sample output from the **show platform software ilpower details** command:

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
    Initialization Done:   Yes
    ILP Supported:         Yes
    ILP Enabled:           Yes
    POST:                  Yes
    Detect On:             No
    Powered Device Detected            No
    Powered Device Class Done          No
    Cisco Powered Device:              No
    Power is On:           No
    Power Denied:          No
    Powered Device Type:               Null
    Powerd Device Class:              Null
    Power State:           NULL
    Current State:         NGWC_ILP_DETECTING_S
    Previous State:        NGWC_ILP_SHUT_OFF_S
    Requested Power in milli watts:       0
    Short Circuit Detected:                 0
    Short Circuit Count:             0
    Cisco Powerd Device Detect Count: 0
    Spare Pair mode:       0
        IEEE Detect:       Stopped
        IEEE Short:        Stopped
        Link Down:         Stopped
        Voltage sense:            Stopped
    Spare Pair Architecture:       1
    Signal Pair Power allocation in milli watts: 0
    Spare Pair Power On:   0
    Powered Device power state:        0
    Timer:
        Power Good:        Stopped
        Power Denied:      Stopped
        Cisco Powered Device Detect:   Stopped
```

show platform software process list

To display the list of running processes on a platform, use the **show platform software process list** command in privileged EXEC mode.

show platform software process list switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**} [**name** *process-name* | **process-id** *process-ID* | **sort memory** | **summary**]

Syntax Description

switch *switch-number*	Displays information about the switch. Valid values for *switch-number* argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the shared port adapters (SPA) Interface Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.
name *process-name*	(Optional) Displays information about the specified process.
process-id *process-ID*	(Optional) Displays information about the specified process ID.
sort	(Optional) Displays information sorted according to processes.
memory	(Optional) Displays information sorted according to memory.
summary	(Optional) Displays a summary of the process memory of the host device.

Command Modes

Privileged EXE (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	The command was introduced.

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

The following is sample output from the **show platform software process list switch active R0** command:

```
Switch# show platform software process list switch active R0 summary

Total number of processes: 278
  Running          : 2
  Sleeping         : 276
  Disk sleeping    : 0
  Zombies          : 0
  Stopped          : 0
  Paging           : 0
```

```
Up time          : 8318
Idle time        : 0
User time        : 216809
Kernel time      : 78931

Virtual memory   : 12933324800
Pages resident   : 634061
Major page faults: 2228
Minor page faults: 3491744

Architecture     : mips64
Memory (kB)
  Physical       : 3976852
  Total          : 3976852
  Used           : 2766952
  Free           : 1209900
  Active         : 2141344
  Inactive       : 1589672
  Inact-dirty    : 0
  Inact-clean    : 0
  Dirty          : 4
  AnonPages      : 1306800
  Bounce         : 0
  Cached         : 1984688
  Commit Limit   : 1988424
  Committed As   : 3358528
  High Total     : 0
  High Free      : 0
  Low Total      : 3976852
  Low Free       : 1209900
  Mapped         : 520528
  NFS Unstable   : 0
  Page Tables    : 17328
  Slab           : 0
  VMmalloc Chunk : 1069542588
  VMmalloc Total : 1069547512
  VMmalloc Used  : 2588
  Writeback      : 0
  HugePages Total: 0
  HugePages Free : 0
  HugePages Rsvd : 0
  HugePage Size  : 2048

Swap (kB)
  Total          : 0
  Used           : 0
  Free           : 0
  Cached         : 0

Buffers (kB)     : 439528

Load Average
  1-Min          : 1.13
  5-Min          : 1.18
  15-Min         : 0.92
```

show platform software process slot switch

To display platform software process switch information, use the **show platform software process slot switch** command in privileged EXEC mode.

show platform software process slot switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**} **monitor** [**cycles** *no-of-times* [**interval** *delay* [**lines** *number*]]]

Syntax Description

switch-number	Switch number.
active	Specifies the active instance.
standby	Specifies the standby instance.
0	Specifies the shared port adapter (SPA) interface processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
R0	Specifies the Route Processor (RP) slot 0.
monitor	Monitors the running processes.
cycles *no-of-tmes*	(Optional) Sets the number of times to run monitor command. Valid values are from 1 to 4294967295. The default is 5.
interval *delay*	(Optional) Sets a delay after each . Valid values are from 0 to 300. The default is 3.
lines *number*	(Optional) Sets the number of lines of output displayed. Valid values are from 0 to 512. The default is 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

The following is sample output from the **show platform software process slot switch active R0 monitor** command:

```
Switch# show platform software process slot switch active R0 monitor
top - 00:01:52 up 1 day, 11:20,  0 users,  load average: 0.50, 0.68, 0.83
```

```
Tasks: 311 total,   2 running, 309 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3955036k used,    21808k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1946764k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 5693 root      20   0  3448 1368  912 R    7  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 186:49.08 fed main event
18662 root      20   0 1806m 678m 263m S    5 17.5 215:32.38 linux_iosd-imag
30276 root      20   0  171m  42m  33m S    5  1.1 125:06.77 repm
17835 root      20   0  935m  74m  63m S    4  1.9  82:28.31 sif_mgr
18534 root      20   0  182m 150m  10m S    2  3.9   8:12.08 smand
    1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
    5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
    7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
    8 root      20   0     0    0    0 S    0  0.0   0:00.00 rcu_bh
    9 root      20   0     0    0    0 S    0  0.0   0:23.08 rcu_sched
   10 root      20   0     0    0    0 S    0  0.0   0:58.04 rcuc/0
   11 root      20   0     0    0    0 S    0  0.0  21:35.60 rcuc/1
   12 root      RT   0     0    0    0 S    0  0.0   0:01.33 migration/1
```

Related Commands

Command	Description
show processes cpu platform monitor location	Displays information about the CPU utilization of the IOS-XE processes.

show platform software status control-processor

To display platform software control-processor status, use the **show platform software status control-processor** command in privileged EXEC mode.

show platform software status control-processor [**brief**]

Syntax Description

brief	(Optional) Displays a summary of the platform control-processor status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

The following is sample output from the **show platform memory software status control-processor** command:

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
  15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.40, System:  1.70, Nice:  0.00, Idle: 93.80
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  3.80, System:  1.20, Nice:  0.00, Idle: 94.90
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  7.00, System:  1.10, Nice:  0.00, Idle: 91.89
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  4.49, System:  0.69, Nice:  0.00, Idle: 94.80
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
  15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2706768 (68%), status: healthy
  Free: 1270084 (32%)
  Committed: 3299332 (83%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  4.50, System:  1.20, Nice:  0.00, Idle: 94.20
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  5.20, System:  0.50, Nice:  0.00, Idle: 94.29
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  3.60, System:  0.70, Nice:  0.00, Idle: 95.69
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  3.00, System:  0.60, Nice:  0.00, Idle: 96.39
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.21, status: healthy, under 5.00
  5-Min: 0.24, status: healthy, under 5.00
  15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1452404 (37%), status: healthy
  Free: 2524448 (63%)
  Committed: 1675120 (42%), under 95%
```

```
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  2.30, System:  0.40, Nice:  0.00, Idle: 97.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.19, System:  0.69, Nice:  0.00, Idle: 95.10
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  4.79, System:  0.79, Nice:  0.00, Idle: 94.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  2.10, System:  0.40, Nice:  0.00, Idle: 97.50
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
  1-Min: 0.20, status: healthy, under 5.00
  5-Min: 0.35, status: healthy, under 5.00
  15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 1451328 (36%), status: healthy
  Free: 2525524 (64%)
  Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.90, System:  0.50, Nice:  0.00, Idle: 97.60
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  4.39, System:  0.19, Nice:  0.00, Idle: 95.40
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
  User:  5.70, System:  1.00, Nice:  0.00, Idle: 93.30
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User:  1.30, System:  0.60, Nice:  0.00, Idle: 98.00
  IRQ:  0.00, SIRQ:  0.10, IOwait:  0.00
```

The following is sample output from the **show platform memory software status control-processor brief** command:

```
Switch# show platform software status control-processor brief

Load Average
 Slot  Status  1-Min  5-Min 15-Min
2-RP0 Healthy   1.10   1.21   0.91
3-RP0 Healthy   0.23   0.27   0.31
4-RP0 Healthy   0.11   0.21   0.22
9-RP0 Healthy   0.10   0.30   0.34

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
2-RP0 Healthy  3976852  2766956 (70%)  1209896 (30%)   3358352 (84%)
3-RP0 Healthy  3976852  2706824 (68%)  1270028 (32%)   3299276 (83%)
4-RP0 Healthy  3976852  1451888 (37%)  2524964 (63%)   1675076 (42%)
9-RP0 Healthy  3976852  1451580 (37%)  2525272 (63%)   1675952 (42%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
2-RP0    0   4.10   2.00   0.00  93.80   0.00   0.10   0.00
         1   4.60   1.00   0.00  94.30   0.00   0.10   0.00
         2   6.50   1.10   0.00  92.40   0.00   0.00   0.00
         3   5.59   1.19   0.00  93.20   0.00   0.00   0.00
3-RP0    0   2.80   1.20   0.00  95.90   0.00   0.10   0.00
         1   4.49   1.29   0.00  94.20   0.00   0.00   0.00
         2   5.30   1.60   0.00  93.10   0.00   0.00   0.00
         3   5.80   1.20   0.00  93.00   0.00   0.00   0.00
4-RP0    0   1.30   0.80   0.00  97.89   0.00   0.00   0.00
         1   1.30   0.20   0.00  98.50   0.00   0.00   0.00
         2   5.60   0.80   0.00  93.59   0.00   0.00   0.00
         3   5.09   0.19   0.00  94.70   0.00   0.00   0.00
```

```
9-RP0    0   3.99   0.69   0.00  95.30   0.00   0.00   0.00
         1   2.60   0.70   0.00  96.70   0.00   0.00   0.00
         2   4.49   0.89   0.00  94.60   0.00   0.00   0.00
         3   2.60   0.20   0.00  97.20   0.00   0.00   0.00
```

show processes cpu platform monitor

To displays information about the CPU utilization of the IOS-XE processes, use the **show processes cpu platform monitor** command in privileged EXEC mode.

show processes cpu platform monitor location switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

Syntax Description

location	Displays information about the Field Replaceable Unit (FRU) location.
switch	Specifies the switch.
switch-number	Switch number.
active	Specifies the active instance.
standby	Specifies the standby instance.
0	Specifies the shared port adapter (SPA) interface processor slot 0.
F0	Specifies the Embedded Service Processor (ESP) slot 0.
R0	Specifies the Route Processor (RP) slot 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

The following is sample output from the **show processes cpu monitor location switch active R0** command:

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22,  0 users,  load average: 0.42, 0.60, 0.78
```

```
Tasks: 312 total,   4 running, 308 sleeping,   0 stopped,   0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3956928k used,    19916k free,   419312k buffers
Swap:        0k total,        0k used,        0k free,  1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
 6294 root      20   0  3448 1368  912 R    9  0.0   0:00.07 top
17546 root      20   0 2044m 244m  79m S    7  6.3 187:02.07 fed main event
30276 root      20   0  171m  42m  33m S    7  1.1 125:15.54 repm
   16 root      20   0     0    0    0 S    5  0.0  22:07.92 rcuc/2
   21 root      20   0     0    0    0 R    5  0.0  22:13.24 rcuc/3
18662 root      20   0 1806m 678m 263m R    5 17.5 215:47.59 linux_iosd-imag
   11 root      20   0     0    0    0 S    4  0.0  21:37.41 rcuc/1
10333 root      20   0  6420 3916 1492 S    4  0.1   4:47.03 btrace_rotate.s
   10 root      20   0     0    0    0 S    2  0.0   0:58.13 rcuc/0
 6304 root      20   0   776   12    0 R    2  0.0   0:00.01 ls
17835 root      20   0  935m  74m  63m S    2  1.9  82:34.07 sif_mgr
    1 root      20   0  8440 4740 2184 S    0  0.1   0:09.52 systemd
    2 root      20   0     0    0    0 S    0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S    0  0.0   0:02.86 ksoftirqd/0
    5 root       0 -20     0    0    0 S    0  0.0   0:00.00 kworker/0:0H
    7 root      RT   0     0    0    0 S    0  0.0   0:01.44 migration/0
```

Related Commands

Command	Description
show platform software process slot switch	Displays platform software process switch information.

show processes memory platform

To display memory usage per Cisco IOS XE process, use the **show processes memory platform** command in privileged EXEC mode.

show processes memory platform [**detailed** {**name** *process-name* | **process-id** *process-ID*} [**location** | **maps** [**location**] | **smaps** [**location**]] | **location** | **sorted** [**location**]] **switch** {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

Syntax Description

detailed *process-name*	(Optional) Displays detailed memory information for a specified Cisco IOS XE process.
name *process-name*	(Optional) Matches the Cisco IOS XE process name.
process-id *process-ID*	(Optional) Matches the Cisco IOS XE process ID.
location	(Optional) Displays information about the FRU location.
maps	(Optional) Displays memory maps of a process.
smaps	(Optional) Displays smaps of a process.

sorted	(Optional) Displays the sorted output based on the total memory used by Cisco IOS XE processes.
switch *switch-number*	Displays information about the device.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the SPA-Inter-Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	The command was introduced.

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

The following is sample output from the **show processes memory platform** command:

```
Switch# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
   Pid    Text      Data   Stack   Dynamic       RSS     Total              Name
--------------------------------------------------------------------------------
     1    1246      4400     132      1308      4400      8328           systemd
    96     233      2796     132       132      2796     12436   systemd-journal
   105     284      1796     132       176      1796      5208     systemd-udevd
   707      52      2660     132       172      2660     11688        in.telnetd
   744     968      3264     132      1700      3264      5800         brelay.sh
   835      52      2660     132       172      2660     11688        in.telnetd
   863     968      3264     132      1700      3264      5800         brelay.sh
   928     968      3996     132      2312      3996      6412      reflector.sh
   933     968      3976     132      2312      3976      6412       droputil.sh
   934     968      2140     132       528      2140      4628            oom.sh
   936     173       936     132       132       936      3068           xinetd
```

```
   945     968      1472     132       132      1472      4168       libvirtd.sh
   947     592     43164     132      3096     43164    154716              repm
   954      45       932     132       132       932      3132           rpcbind
   986     482      3476     132       132      3476    169288          libvirtd
   988      66       940     132       132       940      2724         rpc.statd
   993     968       928     132       132       928      4232   boothelper_evt.
  1017      21       640     132       132       640      2500       inotifywait
  1089     102      1200     132       132      1200      3328        rpc.mountd
  1328       9      2940     132       148      2940     13844             rotee
  1353      39       532     132       132       532      2336             sleep
!
!
!
```

The following is sample output from the **show processes memory platform information** command:

```
Switch# show processes memory platform location switch active R0

System memory: 3976852K total, 2762844K used, 1214008K free,
Lowest: 1214008K
   Pid    Text      Data   Stack   Dynamic       RSS     Total              Name
--------------------------------------------------------------------------------
     1    1246      4400     132      1308      4400      8328           systemd
    96     233      2796     132       132      2796     12436   systemd-journal
   105     284      1796     132       176      1796      5208     systemd-udevd
   707      52      2660     132       172      2660     11688        in.telnetd
   744     968      3264     132      1700      3264      5800         brelay.sh
   835      52      2660     132       172      2660     11688        in.telnetd
   863     968      3264     132      1700      3264      5800         brelay.sh
   928     968      3996     132      2312      3996      6412      reflector.sh
   933     968      3976     132      2312      3976      6412       droputil.sh
!
!
!
```

The following is sample output from the **show processes memory platform sorted** command:

```
Switch# show processes memory platform sorted

System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
   Pid    Text      Data   Stack   Dynamic       RSS     Total              Name
--------------------------------------------------------------------------------
  9655    3787    264964     136     18004    264964   2675968               wcm
 17261     324    248588     132    103908    248588   2093076    fed main event
  7885  149848    684864     136        80    684864   1853548   linux_iosd-imag
 17891     398     75772     136      1888     75772    958240           sif_mgr
 17067    1087     77912     136      1796     77912    702184      platform_mgr
  4268     391    102084     136      5596    102084    482656         cli_agent
  4856     357     93388     132      3680     93388    340052               dbm
 29842    8722     64428     132      8056     64428    297068     fman_fp_image
  5960    9509     76088     136      3200     76088    287156           fman_rp
!
!
!
```

The following is sample output from the **show processes memory platform sorted location switch active R0** command:

```
Switch# show processes memory platform sorted location switch active R0

System memory: 3976852K total, 2763584K used, 1213268K free,
Lowest: 1213268K
   Pid    Text      Data   Stack   Dynamic       RSS     Total              Name
--------------------------------------------------------------------------------
  9655    3787    264968     136     18004    264968   2675968               wcm
 17261     324    249020     132    103908    249020   2093076    fed main event
  7885  149848    684912     136        80    684912   1853548   linux_iosd-imag
 17891     398     75884     136      1888     75884    958240           sif_mgr
 17067    1087     77820     136      1796     77820    702184      platform_mgr
```

```
  4268     391    102084     136      5596    102084    482656         cli_agent
  4856     357     93388     132      3680     93388    340052               dbm
 29842    8722     64428     132      8056     64428    297068     fman_fp_image
  5960    9509     76088     136      3200     76088    287156           fman_rp
!
!
!
```

show power inline

To display the Power over Ethernet (PoE) status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack, use the **show power inline** command in EXEC mode.

show power inline [**police**| **priority**] [*interface-id* | **module** *stack-member-number*] **[detail]**

Syntax Description

police	(Optional) Displays the power policing information about real-time power consumption.
priority	(Optional) Displays the power inline port priority for each port.
interface-id	(Optional) ID of the physical interface.
module *stack-member-number*	(Optional) Limits the display to ports on the specified stack member. The range is 1 to 9. This keyword is supported only on stacking-capable switches.
detail	(Optional) Displays detailed output of the interface or module.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show power inline** command. The table that follows describes the output fields.

```
Device> show power inline
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1             n/a        n/a         n/a
2             n/a        n/a         n/a
3          1440.0       15.4      1424.6
```

```
4           720.0        6.3       713.7
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi3/0/1   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/2   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/3   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/4   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/5   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/6   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/7   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/8   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/9   auto   off        0.0     n/a                 n/a   30.0
Gi3/0/10  auto   off        0.0     n/a                 n/a   30.0
Gi3/0/11  auto   off        0.0     n/a                 n/a   30.0
Gi3/0/12  auto   off        0.0     n/a                 n/a   30.0
<output truncated>
```

This is an example of output from the **show power inline** *interface-id* command on a switch port:

```
Device> show power inline gigabitethernet1/0/1
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   30.0
```

This is an example of output from the **show power inline module** *switch-number* command on stack member 3. The table that follows describes the output fields.

```
Device> show power inline module 3
Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
3           865.0      864.0         1.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi3/0/1   auto   power-deny 4.0     n/a                 n/a   15.4
Gi3/0/2   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/3   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/4   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/5   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/6   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/7   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/8   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/9   auto   off        0.0     n/a                 n/a   15.4
Gi3/0/10  auto   off        0.0     n/a                 n/a   15.4
<output truncated>
```

Table 17: show power inline Field Descriptions

Field	Description
Available	The total amount of configured power[3] on the PoE switch in watts (W).
Used	The amount of configured power that is allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin	Administration mode: auto, off, static.

Field	Description
Oper	Operating mode: • on—The powered device is detected, and power is applied. • off—No PoE is applied. • faulty—Device detection or a powered device is in a faulty state. • power-deny—A powered device is detected, but no PoE is available, or the maximum wattage exceeds the detected powered-device maximum.
Power	The maximum amount of power that is allocated to the powered device in watts. This value is the same as the value in the *Cutoff Power* field in the **show power inline police** command output.
Device	The device type detected: n/a, unknown, Cisco powered-device, IEEE powered-device, or the name from CDP.
Class	The IEEE classification: n/a or a value from 0 to 4.
Max	The maximum amount of power allocated to the powered device in watts.
AdminPowerMax	The maximum amount power allocated to the powered device in watts when the switch polices the real-time power consumption. This value is the same as the *Max* field value.
AdminConsumption	The power consumption of the powered device in watts when the switch polices the real-time power consumption. If policing is disabled, this value is the same as the *AdminPowerMax* field value.

3 The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

This is an example of output from the **show power inline police** command on a stacking-capable switch:

```
Device> show power inline police
Module   Available    Used      Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0        0.0       370.0
3           865.0      864.0         1.0
          Admin  Oper        Admin      Oper       Cutoff Oper
Interface State  State       Police     Police     Power  Power
--------- ------ ----------- ---------- ---------- ------ ------
```

```
Gi1/0/1   auto   off         none       n/a        n/a    0.0
Gi1/0/2   auto   off         log        n/a        5.4    0.0
Gi1/0/3   auto   off         errdisable n/a        5.4    0.0
Gi1/0/4   off    off         none       n/a        n/a    0.0
Gi1/0/5   off    off         log        n/a        5.4    0.0
Gi1/0/6   off    off         errdisable n/a        5.4    0.0
Gi1/0/7   auto   off         none       n/a        n/a    0.0
Gi1/0/8   auto   off         log        n/a        5.4    0.0
Gi1/0/9   auto   on          none       n/a        n/a    5.1
Gi1/0/10  auto   on          log        ok         5.4    4.2
Gi1/0/11  auto   on          log        log        5.4    5.9
Gi1/0/12  auto   on          errdisable ok         5.4    4.2
Gi1/0/13  auto   errdisable  errdisable n/a        5.4    0.0
<output truncated>
```

In the previous example:

- The Gi1/0/1 port is shut down, and policing is not configured.
- The Gi1/0/2 port is shut down, but policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/3 port is shut down, but policing is enabled with a policing action is to shut down the port.
- Device detection is disabled on the Gi1/0/4 port, power is not applied to the port, and policing is disabled.
- Device detection is disabled on the Gi1/0/5 port, and power is not applied to the port, but policing is enabled with a policing action to generate a syslog message.
- Device detection is disabled on the Gi1/0/6 port, and power is not applied to the port, but policing is enabled with a policing action to shut down the port.
- The Gi1/0/7 port is up, and policing is disabled, but the switch does not apply power to the connected device.
- The Gi1/0/8 port is up, and policing is enabled with a policing action to generate a syslog message, but the switch does not apply power to the powered device.
- The Gi1/0/9 port is up and connected to a powered device, and policing is disabled.
- The Gi1/0/10 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/11 port is up and connected to a powered device, and policing is enabled with a policing action to generate a syslog message.
- The Gi1/0/12 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port. The policing action does not take effect because the real-time power consumption is less than the cutoff value.
- The Gi1/0/13 port is up and connected to a powered device, and policing is enabled with a policing action to shut down the port.

This is an example of output from the **show power inline police** *interface-id* command on a standalone switch. The table that follows describes the output fields.

```
Device> show power inline police gigabitethernet1/0/1
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi1/0/1   auto   off        none       n/a        n/a    0.0
```

Table 18: show power inline police Field Descriptions

Field	Description
Available	The total amount of configured power[4] on the switch in watts (W).
Used	The amount of configured power allocated to PoE ports in watts.
Remaining	The amount of configured power in watts that is not allocated to ports in the system. (Available – Used = Remaining)
Admin State	Administration mode: auto, off, static.
Oper State	Operating mode: • errdisable—Policing is enabled. • faulty—Device detection on a powered device is in a faulty state. • off—No PoE is applied. • on—The powered device is detected, and power is applied. • power-deny—A powered device is detected, but no PoE is available, or the real-time power consumption exceeds the maximum power allocation. **Note** The operating mode is the current PoE state for the specified PoE port, the specified stack member, or for all PoE ports on the switch.
Admin Police	Status of the real-time power-consumption policing feature: • errdisable—Policing is enabled, and the switch shuts down the port when the real-time power consumption exceeds the maximum power allocation. • log—Policing is enabled, and the switch generates a syslog message when the real-time power consumption exceeds the maximum power allocation. • none—Policing is disabled.

Field	Description
Oper Police	Policing status: • errdisable—The real-time power consumption exceeds the maximum power allocation, and the switch shuts down the PoE port. • log—The real-time power consumption exceeds the maximum power allocation, and the switch generates a syslog message. • n/a—Device detection is disabled, power is not applied to the PoE port, or no policing action is configured. • ok—Real-time power consumption is less than the maximum power allocation.
Cutoff Power	The maximum power allocated on the port. When the real-time power consumption is greater than this value, the switch takes the configured policing action.
Oper Power	The real-time power consumption of the powered device.

4 The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

show stack-power

To display information about StackPower stacks or switches in a power stack, use the **show stack-power** command in EXEC mode.

{**show stack-power** [**budgeting**| **detail**| **load-shedding**| **neighbors**] [**order** *power-stack-name*]| [**stack-name** [*stack-id*]| **switch** [*switch-id*]]}

Syntax Description

budgeting	(Optional) Displays the stack power budget table.
detail	(Optional) Displays the stack power stack details.
load-shedding	(Optional) Displays the stack power load shedding table.
neighbors	(Optional) Displays the stack power neighbor table.
order *power-stack-name*	(Optional) Displays the load shedding priority for a power stack. **Note** This keyword is available only after the **load-shedding** keyword.

stack-name	(Optional) Displays budget table, details, or neighbors for all power stacks or the specified power stack. **Note** This keyword is not available after the **load-shedding** keyword.
stack-id	(Optional) Power stack ID for the power stack. The stack ID must be 31 characters or less.
switch	(Optional) Displays budget table, details, load-shedding, or neighbors for all switches or the specified switch.
switch-id	(Optional) Switch ID for the switch. The switch number is from 1 to 9.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	Support for all the options was enabled for this command.
Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines

This command is available only on switch stacks running the IP Base or IP Services image.

If a switch is shut down because of load shedding, the output of the **show stack-power** command still includes the MAC address of the shutdown neighbor switch. The command output shows the stack power topology even if there is not enough power to power a switch.

This is an example of output from the **show stack-power** command:

```
Device# show stack-power
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1
```

This is an example of output from the **show stack-power budgeting** command:

```
Device# show stack-power budgeting
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
--------------------  ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  350     150     200     0       1    1

    Power Stack           PS-A   PS-B   Power     Alloc     Avail   Consumd Pwr
SW  Name                  (W)    (W)    Budgt(W)  Power(W)  Pwr(W)  Sys/PoE(W)
--  --------------------  -----  -----  --------  --------  ------  -----------
1   Powerstack-1          350    0      200       200       0       60   /0
--  --------------------  -----  -----  --------  --------  ------  -----------
Totals:                                           200       0       60   /0
```

show stack-power

To display information about StackPower stacks or switches in a power stack, use the **show stack-power** command in EXEC mode.

show stack-power [*power-stack-name*]

Syntax Description

power-stack-name	(Optional) Name of the power stack for which to display power information. The name can be up to 31 characters.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is available only on switch stacks running the IP Base or IP Services image.

If a switch is shut down because of load shedding, the output of the **show stack-power** command still includes the MAC address of the shutdown neighbor switch. The command output shows the stack power topology even if there is not enough power to power a switch.

This is an example of output from the **show stack-power** command:

```
Device# show stack-power
Power Stack           Stack   Stack    Total   Rsvd    Alloc   Unused  Num  Num
Name                  Mode    Topolgy  Pwr(W)  Pwr(W)  Pwr(W)  Pwr(W)  SW   PS
-------------------- ------  -------  ------  ------  ------  ------  ---  ---
Powerstack-1          SP-PS   Stndaln  715     509     190     16      1    1
```

show system mtu

To display the global maximum transmission unit (MTU) or maximum packet size set for the switch, use the **show system mtu** command in privileged EXEC mode.

show system mtu

Syntax Description

This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines For information about the MTU values and the stack configurations that affect the MTU values, see the **system mtu** command.

This is an example of output from the **show system mtu** command:

```
Device# show system mtu
Global Ethernet MTU is 1500 bytes.
```

show tech-support

To automatically run **show** commands that display system information, use the **show tech-support** command in the privilege EXEC mode.

show tech-support [**cef**| **cft**| **eigrp**| **evc**| **fnf**| **ipc**| **ipmulticast**| **ipsec**| **mfib**| **nat**| **nbar**| **onep**| **ospf**| **page**| **password**| **rsvp**| **subscriber**| **vrrp**| **wccp**| **wireless**]

Syntax Description

cef	(Optional) Displays CEF related information.
cft	(Optional) Displays CFT related information.
eigrp	(Optional) Displays EIGRP related information.
evc	(Optional) Displays EVC related information.
fnf	(Optional) Displays flexible netflow related information.
ipc	(Optional) Displays IPC related information.
ipmulticast	(Optional) Displays IP multicast related information.
ipsec	(Optional) Displays IPSEC related information.
mfib	(Optional) Displays MFIB related information.
nat	(Optional) Displays NAT related information.

nbar	(Optional) Displays NBAR related information.
onep	(Optional) Displays ONEP related information.
ospf	(Optional) Displays OSPF related information.
page	(Optional) Displays the command output on a single page at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, it does not stop for page breaks). Press the **Ctrl-C** keys to stop the command output.
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>".
rsvp	(Optional) Displays IP RSVP related information.
subscriber	(Optional) Displays subscriber related information.
vrrp	(Optional) Displays VRRP related information.
wccp	(Optional) Displays WCCP related information.
wireless	(Optional) Displays wireless related information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was enhanced to display of the outputs of the following commands in the output modifier : • **show power inline** • **show platform software ilpower details** • **show power inline police** • **show stack-power budgeting**
Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines

The output from the **show tech-support** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support** > *filename*) in the local writable storage file system or the remote file system. Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

You can use one of the following redirection methods:

- > *filename* - Redirects the output to a file.
- >> *filename* - Redirects the output to a file in append mode.

show wireless interface summary

To display the wireless interface status and configuration, use the **show wireless interface summary** privileged EXEC command.

show wireless interface summary

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This example shows how to display the summary of wireless interfaces:

```
Device# show wireless interface summary
```

speed

To specify the speed of a 10/100 Mb/s or 10/100/1000 Mb/s port, use the **speed** command in interface configuration mode. To return to the default value, use the **no** form of this command.

speed {**10**| **100**| **1000**| **auto** [**10**| **100**| **1000**]| **nonegotiate**}

no speed

Syntax Description

10	Specifies that the port runs at 10 Mb/s.

100	Specifies that the port runs at 100 Mb/s.
1000	Specifies that the port runs at 1000 Mb/s. This option is valid and visible only on 10/100/1000 Mb/s ports.
auto	Automatically detects the speed the port should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds.
nonegotiate	Disables autonegotiation, and the port runs at 1000 Mb/s.

Command Default

The default is **auto**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot configure speed on the 10-Gigabit Ethernet ports.

Except for the 1000BASE-T small form-factor pluggable (SFP) modules, you can configure the speed to not negotiate (**nonegotiate**) when an SFP module port is connected to a device that does not support autonegotiation.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

Caution Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

For guidelines on setting the switch speed and duplex parameters, see the “Configuring Interface Characteristics” chapter in the software configuration guide for this release.

You can verify your settings by entering the **show interfaces** privileged EXEC command.

This example shows how to set speed on a port to 100 Mb/s:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mb/s:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mb/s:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# speed auto 10 100
```

stack-power

To configure StackPower parameters for the power stack or for a switch in the power stack, use the **stack power** command in global configuration mode. To return to the default setting, use the **no** form of the command,

stack-power {**stack** *power-stack-name*| **switch** *stack-member-number*}

no stack-power {**stack** *power-stack-name*| **switch** *stack-member-number*}

Syntax Description

stack *power-stack-name*	Specifies the name of the power stack. The name can be up to 31 characters. Entering these keywords followed by a carriage return enters power stack configuration mode.
switch *stack-member-number*	Specifies the switch number in the stack (1 to 4) to enter switch stack-power configuration mode for the switch.

Command Default

There is no default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **stack-power stack** *power stack name* command, you enter power stack configuration mode, and these commands are available:

- **default—**Returns a command to its default setting.
- **exit—**Exits ARP access-list configuration mode.
- **mode—**Sets the power mode for the power stack. See the **mode** command.
- **no—**Negates a command or returns to default settings.

If you enter the **stack-power switch** *switch-number* command with a switch number that is not participating in StackPower, you receive an error message.

When you enter the **stack-power switch** *switch-number* command with the number of a switch participating in StackPower, you enter switch stack power configuration mode, and these commands are available:

- **default—**Returns a command to its default setting.
- **exit—**Exits switch stack power configuration mode.
- **no—**Negates a command or returns to default settings.
- **power-priority—**Sets the power priority for the switch and the switch ports. See the **power-priority** command.
- **stack-id** *name***—**Enters the name of the power stack to which the switch belongs. If you do not enter the power stack-ID, the switch does not inherit the stack parameters. The name can be up to 31 characters.
- **standalone—**Forces the switch to operate in standalone power mode. This mode shuts down both stack power ports.

This example removes switch 2, which is connected to the power stack, from the power pool and shutting down both power ports:

```
Device(config)# stack-power switch 2
Device(config-switch-stackpower)# standalone
Device(config-switch-stackpower)# exit
```

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

switchport block {**multicast**| **unicast**}

no switchport block {**multicast**| **unicast**}

Syntax Description

multicast	Specifies that unknown multicast traffic should be blocked. **Note** Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.
unicast	Specifies that unknown unicast traffic should be blocked.

Command Default

Unknown multicast and unicast traffic is not blocked.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

For more information about blocking packets, see the software configuration guide for this release.

This example shows how to block unknown unicast traffic on an interface:

```
Device(config-if)# switchport block unicast
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

system mtu

To set the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports, use the **system mtu** command in global configuration mode. To restore the global MTU value to its default value use the **no** form of this command.

system mtu *bytes*

no system mtu

Syntax Description

bytes	The global MTU size in bytes. The range is 1500 to 9198 bytes; the default is 1500 bytes.

Command Default

The default MTU size for all ports is 1500 bytes.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify your setting by entering the **show system mtu** privileged EXEC command.

The switch does not support the MTU on a per-interface basis.

If you enter a value that is outside the allowed range for the specific type of interface, the value is not accepted.

This example shows how to set the global system MTU size to 6000 bytes:

```
Device(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

test mcu read-register

To enable debugging of the Power over Ethernet (PoE) controller, use the **test mcu read-register** command in privileged EXEC mode.

test mcu read-register {**det-cls-offset**| **manufacture-id**| **port-mode**}

Syntax Description

det-cls-offset	Displays the read detection classification register summary.
manufacture-id	Displays the PoE controller manufacture ID.
port-mode	Displays the port mode details.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SECisco IOS XE Denali 16.3.2	This command was introduced.

The following is sample output from the **test mcu read-register det-cls-offset** command:

```
Device# test mcu read-register det-cls-offset 1
 DETECTION ENABLE BIT SUMMARY

Controller    port1          port2          port3          port4       register
                                                                     (hexadecimal)
----------   -------        -------        -------        -------    ------------
1               1              0              1              0            5

2               1              0              1              0            5

3               1              0              1              0            5

4               1              0              1              0            5
```

```
5               1              0              1              0            5
6               1              0              1              0            5
7               1              0              1              0            5
8               1              0              1              0            5
9               1              0              1              0            5
10              1              0              1              0            5
11              0              0              1              0            4
12              1              0              0              0            1
 CLASSIFICATION ENABLE BIT SUMMARY
Controller    port1          port2          port3          port4       register
                                                                     (hexadecimal)
----------   -------        -------        -------        -------    ------------
1               1              0              1              0            5
2               1              0              1              0            5
3               1              0              1              0            5
4               1              0              1              0            5
5               1              0              1              0            5
6               1              0              1              0            5
7               1              0              1              0            5
8               1              0              1              0            5
9               1              0              1              0            5
10              1              0              1              0            5
11              0              0              1              0            4
12              1              0              0              0            1
```

The following is sample output from the **test mcu read-register manufacture-id** command:

```
MANUFACTURE ID : DEVICE_BCM_PALPATINE reg_val = 0x1B
```

The following is sample output from the **test mcu read-register port-mode** command:

```
 PORT MODE SUMMERY
Controller    port1          port2          port3          port4       register
                                                                     (hexadecimal)
----------   -------        -------        -------        -------    ------------
1              01             00             01             00           22
2              01             00             01             00           22
3              01             00             01             00           22
4              01             00             01             00           22
5              01             00             01             00           22
6              01             00             01             00           22
7              01             00             01             00           22
8              01             00             01             00           22
9              01             00             01             00           22
```

```
10          01          00          01          00          22
11          00          00          01          00          20
12          01          00          00          00           2
```

voice-signaling vlan (network-policy configuration)

To create a network-policy profile for the voice-signaling application type, use the **voice-signaling vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

voice-signaling vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos *cos-value*	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp *dscp-value*	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice-signaling application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice-signaling application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the voice policy TLV.

When you are in network-policy profile configuration mode, you can create the profile for voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure voice-signaling for VLAN 200 with a priority 2 CoS:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 200 cos 2
```

This example shows how to configure voice-signaling for VLAN 400 with a DSCP value of 45:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 400 dscp 45
```

This example shows how to configure voice-signaling for the native VLAN with priority tagging:

```
Device(config-network-policy)# voice-signaling vlan dot1p cos 4
```

voice vlan (network-policy configuration)

To create a network-policy profile for the voice application type, use the **voice vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

voice vlan {*vlan-id* [**cos** *cos-value*| **dscp** *dscp-value*]| **dot1p** [**cos** *l2-priority*| **dscp** *dscp*]| **none**| **untagged**}

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos *cos-value*	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp *dscp-value*	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.

untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

When you are in network-policy profile configuration mode, you can create the profile for voice by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

```
Device(config-network-policy)# voice vlan dot1p cos 4
```

wireless ap-manager interface

To configure the wireless AP-manager interface, use the **wireless ap-manager interface** command.

wireless ap-managerinterface {**TenGigabitEthernet** *interface-number*| **Vlan** *interface-number*}

Syntax Description

TenGigabitEthernet *interface-name*	Configures 10-Gigabit Ethernet interface. Values range from 0 to 9.
Vlan *interface-name*	Configures VLANs. Values range from 1 to 4095.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the wireless AP-manager:

```
Device# wireless ap-manager interface vlan
<1-4095>  Vlan interface number
```

This example shows how to configure the wireless AP-manager:

```
Device# #wireless ap-manager interface vlan 10
```

wireless exclusionlist

To manage exclusion list entries, use the **wireless exclusionlist** global configuration command. To remove the exclusion list entries, use the **no** form of the command.

wireless exclusionlist *mac-addr* **description** *description*

no wireless exclusionlist *mac-addr*

Syntax Description

mac-addr	The MAC address of the local excluded entry.
description *description*	Specifies the description for an exclusion-list entry.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to create a local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Device# wireless exclusionlist xxx.xxx.xxx
```

This example shows how to create a description for the local exclusion list entry for the MAC address xxx.xxx.xxx:

```
Device# wireless exclusionlist xxx.xxx.xxx description sample
```

wireless linktest

To configure linktest frame size and number of frames to send, use the **wireless linktest** command.

wireless linktest {**frame-size** *size*| **number-of-frames** *value*}

Syntax Description

frame-size *size*	Specifies the link test frame size for each packet. The values range from 1 to 1400.
number-of-frames *value*	Specifies the number of frames to be sent for the link test. The values range from 1 to 100.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the link test frame size of each frame as 10:

```
Device# wireless linktest frame-size 10
```

wireless management interface

To configure wireless management parameters on an interface, use the **wireless management interface** global configuration command. To remove a wireless management parameters on an interface, use the **no** form of the command.

wireless management interface *interface-name* {**TenGigabitEthernet** *interface-name*| **Vlan** *interface-name*}

no wireless management interface

Syntax Description

interface-name	The interface number.
TenGigabitEthernet *interface-name*	The 10-Gigabit Ethernet interface number. The values range from 0 to 9.
Vlan *interface-name*	The VLAN interface number. The values range from 1 to 4095.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure VLAN 10 on the wireless interface:

```
Device# wireless management interface Vlan 10
```

wireless peer-blocking forward-upstream

To configure peer-to-peer blocking for forward upstream, use the **wireless peer-blocking forward-upstream** command. To remove a peer-to-peer blocking, use the **no** form of the command.

wireless peer-blocking forward-upstream *interface*{**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

no wireless peer-blocking forward-upstream {**GigabitEthernet** *interface-number* **TenGigabitEthernet** *interface-number*}

Syntax Description

GigabitEthernet *interface*	The Gigabit Ethernet interface number. Values range from 0 to 9.

TenGigabitEthernet *interface*	The 10-Gigabit Ethernet interface number. Values range from 0 to 9.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure peer-to-peer blocking for interface 10-gigabit ethernet interface:

```
Device(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```

PART IV

IP Multicast Routing Commands

- IP Multicast Commands, page 211

CHAPTER 5

IP Multicast Commands

- cache-memory-max, page 212
- clear ip mfib counters, page 213
- clear ip mroute, page 214
- ip igmp filter, page 215
- ip igmp max-groups, page 216
- ip igmp profile, page 218
- ip igmp snooping, page 219
- ip igmp snooping last-member-query-count, page 220
- ip igmp snooping querier, page 221
- ip igmp snooping report-suppression, page 223
- ip igmp snooping vlan mrouter, page 224
- ip igmp snooping vlan static, page 225
- ip multicast auto-enable, page 226
- ip multicast vlan, page 226
- ip pim accept-register, page 227
- ip pim bsr-candidate, page 228
- ip pim rp-candidate, page 230
- ip pim send-rp-announce, page 231
- ip pim spt-threshold, page 232
- match message-type, page 233
- match service-type, page 234
- match service-instance, page 234
- mrinfo, page 235
- redistribute mdns-sd, page 236

- service-list mdns-sd, page 237
- service-policy-query, page 238
- service-routing mdns-sd, page 239
- service-policy, page 240
- show ip igmp filter, page 240
- show ip igmp profile, page 241
- show ip igmp snooping, page 242
- show ip igmp snooping groups, page 244
- show ip igmp snooping igmpv2-tracking, page 245
- show ip igmp snooping mrouter, page 245
- show ip igmp snooping querier, page 246
- show ip igmp snooping wireless mcast-spi-count, page 248
- show ip igmp snooping wireless mgid, page 248
- show ip pim autorp, page 249
- show ip pim bsr-router, page 250
- show ip pim bsr, page 251
- show ip pim tunnel, page 252
- show mdns cache, page 253
- show mdns requests, page 254
- show mdns statistics, page 255
- show platform ip multicast, page 256
- wireless mdns-bridging, page 263
- wireless multicast, page 263

cache-memory-max

To set a percentage of the system memory for cache, use the **cache-memory-max** command. To remove a percentage of system memory for cache, use the **no** form of this command.

cache-memory-max *cache-config-percentage*

no cache-memory-max *cache-config-percentage*

Syntax Description

cache-config-percentage	A percentage of the system memory for cache.

Command Default 10 percent.

Command Modes mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines The number of services learned in a network could be large, so there is an upper limit on the amount of cache memory that can be used. The memory is set by default to a maximum of 10 percent of the system memory.

Note You can override the default value by using this command.

When you try to add new records, and the cache is full, the records in the cache that are close to expiring are deleted to provide space for the new records.

Example

This example sets 20 percent of the system memory for cache:

```
Device(config-mdns)# cache-memory-max 20
```

clear ip mfib counters

To clear all active IPV4 multicast forwarding information base (MFIB) traffic counters, use the **clear ip mfib counters** privileged exec command.

clear ip mfib [**global** | **vrf ***] **counters** [*group-address*] [*hostname* | *source-address*]

Syntax Description

global	(Optional) Resets the IP multicast forwarding information base cache to the global default configuration.
vrf *	(Optional) Clears the IP multicast forwarding information base cache for all VPN routing and forwarding instances.
group-address	(Optional) Limits the active multicast forwarding information base (MFIB) traffic counters to the indicated group address.
hostname | *source-address*	(Optional) Limits the active multicast forwarding information base (MFIB) traffic counters to the indicated host name or source address.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines None

Examples

The following example shows how to reset all active MFIB traffic counters for all multicast tables:

```
Device# clear ip mfib counters
```

The following example shows how to reset the IP multicast forwarding information base cache counters to the global default configuration:

```
Device# clear ip mfib global counters
```

The following example shows how to clear the IP multicast forwarding information base cache for the all VPN routing and forwarding instances:

```
Device# clear ip mfib vrf * counters
```

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** privileged EXEC command.

clear ip mroute [**vrf** *vrf-name*]{***** | *ip-address* | *group-address*}[*hostname* | *source-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
*****	Specifies all Multicast routes.
ip-address	Multicast routes for the IP address.
group-address	Multicast routes for the group address.
hostname	(Optional) Multicast routes for the host name.
source-address	(Optional) Multicast routes for the source address.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Examples

The following example shows how to delete all entries from the IP multicast routing table:

```
Device# clear ip mroute *
```

The following example shows how to delete all sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
Device# clear ip mroute 224.2.205.42 228.3.0.0
```

ip igmp filter

To control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface, use the **ip igmp filter** interface configuration command on the device stack or on a standalone device. To remove the specified profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*

no ip igmp filter

Syntax Description

profile number	The IGMP profile number to be applied. The range is 1 to 4294967295.

Command Default No IGMP filters are applied.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more device port interfaces, but one port can have only one profile applied to it.

Example

This example shows how to configure IGMP profile 40 to permit the specified range of IP multicast addresses, then shows how to apply that profile to a port as a filter:

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Device(config-igmp-profile)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport
*Jan  3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply the
 filter.
Device(config-if)# ip igmp filter 40
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp max-groups

To set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table, use the **ip igmp max-groups** interface configuration command on the device stack or on a standalone device. To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

ip igmp max-groups {*max number* | **action** { **deny** | **replace**}}

no ip igmp max-groups {*max number* | **action**}

Syntax Description

max number	The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit.
action deny	Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.

action replace	Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the IGMP snooping forwarding table.

Command Default

The default maximum number of groups is no limit.

After the device learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the device drops the next IGMP report received on the interface.
- If you configure the throttling action as replace and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the device replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
```

This example shows how to configure the device to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command on the device stack or on a standalone device. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

ip igmp profile *profile number*

no ip igmp profile *profile number*

Syntax Description

profile number	The IGMP profile number being configured. The range is from 1 to 4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny—**Specifies that matching addresses are denied; this is the default condition.
- **exit—**Exits from igmp-profile configuration mode.
- **no—**Negates a command or resets to its defaults.
- **permit—**Specifies that matching addresses are permitted.
- **range—**Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Example

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses:

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the device or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the device stack or on a standalone device. To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.

Command Default

IGMP snooping is globally enabled on the device.

IGMP snooping is enabled on VLAN interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable IGMP snooping:

```
Device(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Device(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of the command.

ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

no ip igmp snooping [**vlan** *vlan-id*] **last-member-query-count** *count*

Syntax Description

vlan *vlan-id*	(Optional) Sets the count value on a specific VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
count	The interval at which query messages are sent, in milliseconds. The range is from 1 to 7. The default is 2.

Command Default

A query is sent every 2 milliseconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response to the last-member queries are received before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.

Note Do not set the count to 1 because the loss of a single packet (the query packet from the device to the host or the report packet from the host to the device) may result in traffic forwarding being stopped even if there is still a receiver. Traffic continues to be forwarded after the next general query is sent by the device, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last-member-query-interval (LMQI) value when the device is processing more than one leave within an LMQI. In this case, the average leave latency is determined by the (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

The following example sets the last member query count to 5:

```
Device(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** {**count** *count* | **interval** *interval*} | **timer expiry** *expiry-time* | **version** *version*]

no ip igmp snooping [**vlan** *vlan-id*] **querier** [**address** | **max-response-time** | **query-interval** | **tcn query** {**count** | **interval**} | **timer expiry** | **version**]

Syntax Description

vlan *vlan-id*	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
address *ip-address*	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.
max-response-time *response-time*	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds.
query-interval *interval-count*	(Optional) Sets the interval between IGMP queriers. The range is 1 to 18000 seconds.
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).
count *count*	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.
interval *interval*	Sets the TCN query interval time. The range is 1 to 255.
timer expiry *expiry-time*	(Optional) Sets the length of time until the IGMP querier expires. The range is 60 to 300 seconds.

version *version*	(Optional) Selects the IGMP version number that the querier feature uses. Select 1 or 2.

Command Default

The IGMP snooping querier feature is globally disabled on the device.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2) but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the max-response-time value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the max-response-time value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Device(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Device(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Device(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Device(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Device(config)# ip igmp snooping querier timer expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Device(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the device stack or on a standalone device. To disable IGMP report suppression and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

IGMP report suppression is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all hosts for a group to all the multicast routers. The device does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the device forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the device forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Example

This example shows how to disable report suppression:

```
Device(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the device stack or on a standalone device. To return to the default settings, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id*}

Syntax Description

vlan-id	Enables IGMP snooping, and adds the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094.
interface *interface-id*	Specifies the next-hop interface to the multicast router. The arguments have these meanings: • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0 to 128.

Command Default

By default, there are no multicast router ports.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Examples

This example shows how to configure a port as a multicast router port:

```
Device(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the device stack or on a standalone device. Use the **no** form of this command to remove ports specified as members of a static multicast group.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

vlan-id	Enables IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094.
ip-address	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface *interface-id*	Specifies the interface of the member port. The *interface-id* value has these options: • *fastethernet interface number*—A Fast Ethernet IEEE 802.3 interface. • *gigabitethernet interface number*—A Gigabit Ethernet IEEE 802.3z interface. • *tengigabitethernet interface number*—A 10-Gigabit Ethernet IEEE 802.3z interface. • *port-channel interface number*—A channel interface. The range is 0 to 128.

Command Default

By default, there are no ports statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

This example shows how to statically configure a host on an interface:

```
Device(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
Configuring port gigabitethernet1/0/1 on group 224.2.4.12
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of the command.

ip multicast auto-enable

no ip multicast auto-enable

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

This command is unavailable when using the LAN Base image.

Example

This example shows how to enable authentication, authorization, and accounting (AAA) on IP multicast:

```
Device(config)# ip multicast auto-enable
```

ip multicast vlan

To configure IP multicast on a single VLAN, use the **ip multicast vlan** command in global configuration mode. To remove the VLAN from the WLAN, use the **no** form of the command.

ip multicast vlan {*vlan-name* | *vlan-id*}

no ip multicast vlan {*vlan-name* | *vlan-id*}

Syntax Description

vlan-name	Specifies the VLAN name.
vlan-id	Specifies the VLAN ID.

Command Default

Disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

This example configures vlan_id01 as a multicast VLAN.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan 1
Device(config-wlan)# ip multicast vlan vlan_id01
```

ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list*}

no ip pim [**vrf** *vrf-name*] **accept-register**

Syntax Description

vrf *vrf-name*	(Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
list *access-list*	Specifies the *access-list* argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100 to 199 and an expanded range of 2000 to 2699. An IP-named access list can also be used.

Command Default

No PIM register filters are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list provided for the **ip pim accept-register** command should only filter on IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is desired, use the **ip multicast boundary** command instead.

Example

The following example shows how to permit register packets for any source address sending to any group range, with the exception of source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). These are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers or switches.

```
Device(config)# ip pim accept-register list ssm-range
Device(config)# ip access-list extended ssm-range
Device(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
Device(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

To configure the switch to be a candidate BSR, use the **ip pim bsr-candidate** command in global configuration mode. To remove the switch as a candidate BSR, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-id* [*hash-mask-length*] [*priority*]

no ip pim [**vrf** *vrf-name*] **bsr-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configures the switch to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-id	ID of the interface on this switch from which the BSR address is derived to make it a candidate. This interface must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command. Valid interfaces include physical ports, port channels, and VLANs.

hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.

Command Default

The switch is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the switch to send BSR messages to all of its PIM neighbors, with the address of the designated interface as the BSR address.

This command should be configured on backbone switches that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) switches unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so no preexisting IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each switch that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Cisco switches always accept and process BSR messages. There is no command to disable this function.

Cisco switches perform the following steps to determine which C-RP is used for a group:

- A longest match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP are found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
- If more than one BSR-learned C-RP have the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP return the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

Example

The following example shows how to configure the IP address of the switch on Gigabit Ethernet interface 1/0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Device(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

To configure the switch to advertise itself to the BSR as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this switch as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

no ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-id* [**group-list** *access-list-number*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-id	ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

Command Default

The switch is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure the switch to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.

This command should be configured on backbone switches that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified by *interface-id* will be advertised as the C-RP address.

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list-number* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.

Example

The following example shows how to configure the switch to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 1/0/1.

```
Device(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

To use Auto-RP to configure groups for which the switch will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this switch as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id* **scope** *ttl-value* [**group-list** *access-list-number*] [**interval** *seconds*]

no ip pim [**vrf** *vrf-name*] **send-rp-announce** *interface-id*

Syntax Description

vrf *vrf-name*	(Optional) Uses Auto-RP to configure groups for which the switch will act as a rendezvous point (RP) for the *vrf-name* argument.
interface-id	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.
scope *ttl-value*	Specifies the time-to-live (TTL) value in hops that limits the number of Auto-RP announcements. Enter a hop count that is high enough so that the RP-announce messages reach all mapping agents in the network. There is no default setting. The range is 1 to 255.
group-list *access-list-number*	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1 to 99. If no access list is configured, the RP is used for all groups.
interval *seconds*	(Optional) Specifies the interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1 to 16383.

Command Default

Auto-RP is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enter this command on the switch that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

Examples

The following example shows how to configure the switch to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the switch wants to be identified as RP is the IP address associated with Gigabit Ethernet interface 1/0/1 at an interval of 120 seconds:

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval
 120
```

ip pim spt-threshold

To specify the threshold that must be reached before moving to shortest-path tree (spt), use the **ip pim spt-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim {*kbps* | **infinity**} [**group-list** *access-list*]

Syntax Description

kbps	The threshold that must be reached before moving to shortest-path tree (spt). 0 is the only valid entry even though the range is 0 to 4294967. A 0 entry always switches to the source-tree.
infinity	Specifies that all sources for the specified group use the shared tree, never switching to the source tree.
group-list *access-list*	(Optional) Specifies an access list number or a specific access list that you have created by name. If the value is 0 or if the **group-list** *access-list* option is not used, the threshold applies to all groups.

Command Default

Switches to the PIM shortest-path tree (spt).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Example

The following example makes all sources for access list 16 use the shared tree:

```
Device(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

To set the message type to match for a service list, use the **match message-type** command.

match message-type {**announcement**| **any**| **query**}

Syntax Description

announcement	Allows only service advertisements or announcements for the device.
any	Allows any match type.
query	Allows only a query from the client for a certain device in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each one has a permit or deny result. Evaluation of service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and an action permit/deny associated with the statement match is performed. The default action after scanning through the entire list is to deny.

Note It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

This example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl)# match message-type announcement
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type *line*

Syntax Description

line	Regular expression to match service type in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

This example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

To set the service instance to match for a service list, use the **match service-instance** command.

match servcie-instance *line*

Syntax Description

line	Regular expression to match service instance in packets.

Command Default

None

Command Modes

Service list configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

It is not possible to use the **match** command if you have used the **service-list mdns-sd** *service-list-name* **query** command. The **match** command can be used only for the **permit** or **deny** option.

This example shows how to set the service instance to match:

```
Device(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

To query which neighboring multicast routers or multilayer switches are acting as peers, use the **mrinfo** command in user EXEC or privileged EXEC mode.

mrinfo [**vrf** *route-name*] [*hostname* | *address*][*interface-id*]

Syntax Description

vrf *route-name*	(Optional) Specifies the VPN routing or forwarding instance.
hostname | *address*	(Optional) The Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
interface-id	(Optional) Specifies the interface ID.

Command Default

The command is disabled.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers have supported responding to mrinfo requests since Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Example

The following is sample output from the **mrinfo** command:

```
Device# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

Note The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol (SNMP)-capable
- A: Auto-Rendezvous Point (RP)-capable

redistribute mdns-sd

To redistribute services or service announcements across subnets, use the **redistribute mdns-sd** command. To disable redistribution of services or service announcements across subnets, use the **no** form of this command.

redistribute mdns-sd

no redistribute mdns-sd

This command has no arguments or keywords.

Command Default

The redistribution of services or service announcements across subnets is disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

To redistribute service announcements across interfaces, use the **redistribute mdns-sd** command. This command sends out unsolicited announcements received on one interface to all of the other interfaces. The outgoing announcements are filtered as per the out-service policy defined for the interface or in absence of a per-interface service policy based on the global out-service policy.

In the absence of a redistribute option, services can be discovered by querying in a Layer 3 domain that is not local to the service provider.

Example

This example shows how to redistribute services or service announcements across subnets:

```
Device(config-mdns)# redistribute mdns-sd
```

Note If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

service-list mdns-sd

To enter mDNS service discovery service-list mode on the device, use the **service-list mdns-sd** command. To exit mDNS service discovery service-list mode, use the **no** form of the command.

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

Syntax Description

service-list-name	Name of the service list.
permit *sequence number*	Permits a filter on the service list to be applied to the sequence number.
deny *sequence number*	Denies a filter on the service list to be applied to the sequence number.
query	Associates a query for the service list name.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Service filters are modeled around access lists and route maps.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, each has a permit or deny result. Evaluation of a service list consists of a list scan, in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is aborted once the first statement match is found and an action, permit or deny associated with the statement match is performed. Default action after scanning through the entire list will be to deny.

This command can be used to enter mDNS service discovery service-list mode.

In this mode you can:

- Create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number.

Example

This example shows how to create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number:

```
Device(config)# service-list mdns-sd sl1 permit 3
```

service-policy-query

To configure service list query periodicity, use the **service-policy-query** command. To delete the configuration, use the **no** form of this command.

service-policy-query [*service-list-query-name service-list-query-periodicity*]

no service-policy-query

Syntax Description

service-list-query-name service-list-query-periodicity	(Optional) Configures the service list query periodicity.

Command Default

Disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

As there are devices that do not send unsolicited announcements and to force learning of services and to keep them refreshed in the cache, this command contains an active query feature which ensures that services listed in the active query list will be queried.

Example

This example shows how to configure service list query periodicity:

```
Device(config-mdns)# service-policy-query sl-query1 100
```

service-routing mdns-sd

To enable mDNS gateway functionality for a device and enter multicast DNS configuration mode, use the **service-routing mdns-sd** command. To restore default settings and return to global config mode, enter the **no** form of the command.

service-routing mdns-sd

no service-routing mdns-sd

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

mDNS gateway functionality can only be enabled or disabled globally, not on a per-interface basis. The service filter policy and redistribution can be configured globally as well as on a per-interface basis. Any interface specific configuration overrides the global configuration.

Example

This example shows how to enable mDNS gateway functionality for a device and enter multicast DNS configuration mode:

```
Device(config)# service-routing mdns-sd
```

service-policy

To apply a filter on incoming or outgoing service discovery information on a service list, use the **service-policy** command. To remove the filter, use the **no** form of the command.

service-policy *service-policy-name* {**IN** | **OUT**}

no service-policy *service-policy-name* {**IN** | **OUT**}

Syntax Description

service-policy-name **IN**	Applies a filter on incoming service discovery information.
service-policy-name **OUT**	Applies a filter on outgoing service discovery information.

Command Default

Disabled.

Command Modes

mDNS configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The Device intercepts mDNS packets. If they are mDNS messages destined to a wireless client (for example, the destination MAC is client's MAC address), and the client's mobility state is either local or foreign, the destination MAC address is overwritten with the client's MAC address and enqueues the packet to be sent out on the associated CAPWAP tunnel.

Example

This example applies a filter on incoming service discovery information on a service list:

```
Device(config-mdns)#  service-policy serv-pol1 IN
```

show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the **show ip igmp filter** command in privileged EXEC command mode.

show ip igmp [**vrf** *vrf-name*] **filter**

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.

Command Default

IGMP filters are enabled by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show ip igmp filter** command displays information about all filters defined on the device.

Example

The following is sample output from the **show ip igmp filter** command:

```
Device# show ip igmp filter
IGMP filter enabled
```

show ip igmp profile

To display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** privileged EXEC command.

show ip igmp [**vrf** *vrf-name*] **profile** [*profile number*]

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
profile number	(Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed.

Command Default

IGMP profiles undefined by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example shows the output of the **show ip igmp profile** privileged EXEC command for profile number 40 on the device:

```
Device# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255
```

This example shows the output of the **show ip igmp profile** privileged EXEC command for all profiles configured on the device:

```
Device# show ip igmp profile

IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the device or the VLAN, use the **show ip igmp snooping** command in user or privileged EXEC command mode.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description

groups	(Optional) Displays the IGMP snooping multicast table.
mrouter	(Optional) Displays the IGMP snooping multicast router ports.
querier	(Optional) Displays the configuration and operation information for the IGMP querier.
vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Device# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
CGMP interoperability mode           : IGMP_ONLY
Robustness variable                  : 2
Last member query count              : 2
Last member query interval           : 1000
```

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the device:

```
Device# show ip igmp snooping
Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Multicast router learning mode       : pim-dvmrp
```

```
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
Vlan 2:
--------
IGMP snooping                       : Enabled
IGMPv2 immediate leave              : Disabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000
<output truncated>
```

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the device or the multicast information, use the **show ip igmp snooping groups** privileged EXEC command.

show ip igmp snooping groups [**vlan** *vlan-id*] [[**count**] | *ip_address*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
ip_address	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the device:

```
Device# show ip igmp snooping groups
Vlan      Group          Type        Version     Port List
```

```
-------------------------------------------------------------
1         224.1.4.4      igmp                    Gi1/0/11
1         224.1.4.5      igmp                    Gi1/0/11
2         224.0.1.40     igmp        v2          Gi1/0/15
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi2/0/2
104       224.1.4.3      igmp        v2          Gi2/0/1, Gi2/0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the device:

```
Device# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Device# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group          Type        Version     Port List
-------------------------------------------------------------
104       224.1.4.2      igmp        v2          Gi2/0/1, Gi1/0/15
```

show ip igmp snooping igmpv2-tracking

To display group and IP address entries, use the **show ip igmp snooping igmpv2-tracking** command in privileged EXEC mode.

Note The command displays group and IP address entries only for wireless multicast IGMP joins and not for wired joins. This command also displays output only if wireless multicast is enabled.

show ip igmp snooping igmpv2-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the device or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** privileged EXEC command.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Example

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the device:

```
Device# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi2/0/1(dynamic)
```

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier configured on a device, use the **show ip igmp snooping querier** user EXEC command.

show ip igmp snooping querier [**vlan** *vlan-id*] [**detail**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays detailed IGMP querier information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 device.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier is learned in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain Output appear.

Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
--------------------------------------------------
1         172.20.50.11   v3                  Gi1/0/1
2         172.20.40.20   v2                  Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Device> show ip igmp snooping querier detail
Vlan      IP Address     IGMP Version   Port
-------------------------------------------------------------
1         1.1.1.1        v2             Fa8/0/1
Global IGMP device querier status
-------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
Vlan 1:   IGMP device querier status
-------------------------------------------------------
elected querier is 1.1.1.1         on port Fa8/0/1
```

```
-------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

show ip igmp snooping wireless mcast-spi-count

To display the statistics of the number of multicast stateful packet inspections (SPIs) per multicast group ID (MGID) sent to the device, use the **show ip igmp snooping wireless mcast-spi-count** command in privileged EXEC mode.

show ip igmp snooping wireless mcast-spi-count

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mcast-spi-count** command:

```
Device# show ip igmp snooping wireless mcast-spi-count

Stats for Mcast Client Add/Delete SPI Messages Sent to WCM

MGID    ADD MSGs        Del MSGs
--------------------------------
4160    1323            667
```

show ip igmp snooping wireless mgid

To display multicast group ID (MGID) mappings, use the **show ip igmp snooping wireless mgid** command in privileged EXEC mode.

show ip igmp snooping wireless mgid

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This is an example of output from the **show ip igmp snooping wireless mgid** command:

```
Device# show ip igmp snooping wireless mgid

Total number of L2-MGIDs    = 0

Total number of MCAST MGIDs = 0

 Wireless multicast is Enabled in the system
 Vlan     bcast   nonip-mcast   mcast    mgid    Stdby Flags
 1     Disabled   Disabled   Enabled    Disabled  0:0:1:0
 25    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 34    Disabled   Disabled   Enabled    Disabled  0:0:1:0
 200   Disabled   Disabled   Enabled    Disabled  0:0:1:0
 1002  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1003  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1004  Enabled    Enabled    Enabled    Disabled  0:0:1:0
 1005  Enabled    Enabled    Enabled    Disabled  0:0:1:0

Index  MGID                  (S, G, V)
-----------------------------------------------------------
```

show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

show ip pim autorp

Syntax Description

This command has no arguments or keywords.

Command Default

auto-rp is enabled by default.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command displays whether auto-rp is enabled or disabled.

Example

The following command output displays that auto-rp is enabled:

```
Device# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim bsr-router

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In addition to auto-rp, the BSR RP method can be configured. After the BSR RP method is configured, this command will display the BSR router information.

The following is sample output from the **show ip pim bsr-router** command:

```
Device# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

show ip pim bsr

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In addition to auto-rp, the BSR RP method can be configured. After the BSR RP method is configured, this command will display the BSR router information.

The following is sample output from the **show ip pim bsr** command:

```
Device# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and decapsulation tunnels on an interface, use the **show ip pim tunnel** command.

show ip pim [**vrf** *vrf-name*] **tunnel** [**Tunnel** *interface-number* | **verbose**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
Tunnel *interface-number*	(Optional) Specifies the tunnel interface number.
verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip pim tunnel** to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel)

The PIM Encap Tunnel is dynamically created whenever a group-to-rendezvous point (RP) mapping is learned (through auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop designated routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created—but it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.

Note PIM tunnels will not appear in the running configuration.

The following syslog message appears when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

The following is sample output from the **show ip pim tunnel** taken from an RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP:

```
Device# show ip pim tunnel

Tunnel0
   Type  : PIM Encap
  RP    : 70.70.70.1*
  Source: 70.70.70.1
Tunnel1*
  Type  : PIM Decap
  RP    : 70.70.70.1*
  Source: -R2#
```

Note The asterisk (*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

show mdns cache

To display mDNS cache information for the device, use the **show mdns cache** privileged EXEC command.

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

Syntax Description

interface *type-number*	(Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.
name *record-name*	(Optional) Specifies a particular name for which mDNS cache information is to be displayed.
type *record-type*	(Optional) Specifies a particular type for which mDNS cache information is to be displayed.

Command Default

None

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

Example

This is an example of output from the **show mdns cache** command without any keywords:

```
Device# show mdns cache

==========================================================================================
[<NAME>]                          [<TYPE>][<CLASS>][<TTL>/Remaining][Accessed][If-name][Mac
 Address][<RR Record Data>]

_airplay._tcp.local                  PTR     IN      4500/4455         0        Vl121
b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

CAMPUS APPLE TV1._airplay._tcp.local SRV     IN      120/75            2        Vl121
b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

CAMPUS-APPLE-TV1.local               A       IN      120/75            2        Vl121
b878.2e33.c7c5  121.1.0.254

CAMPUS APPLE TV1._airplay._tcp.local TXT     IN      4500/4455         2        Vl121
b878.2e33.c7c5  (162) 'deviceid=B8:78:2E:33:C7:C6'

              'features=0x5a7ffff7''flags=0x4'

              'model=AppleT~'~

_ipp._tcp.local                      PTR     IN      4500/4465         2        Vl2
2894.0fed.447f  EPSON XP-400 Series._ipp._tcp.local

EPSON XP-400 Series._ipp._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSONC053AA.local                    A       IN      120/85            2        Vl2
2894.0fed.447f  121.1.0.251

EPSON XP-400 Series._ipp._tcp.local  TXT     IN      4500/4465         2        Vl2
2894.0fed.447f  (384)'txtvers=1' N XP-400 Series'

              'usbFG=EPSON''usb_MDL=XP~'~

_smb._tcp.local                      PTR     IN      4500/4465         2        Vl2
2894.0fed.447f  EPSON XP-400 Series._smb._tcp.local

EPSON XP-400 Series._smb._tcp.local  SRV     IN      120/85            2        Vl2
2894.0fed.447f  EPSONC053AA.local

EPSON XP-400 Series._smb._tcp.local  TXT     IN      4500/4465         2        Vl2
2894.0fed.447f  (1)'' R2-Access1#
```

show mdns requests

To display information for outstanding mDNS requests, including record name and record type information, for the device, use the **show mdns requests** privileged EXEC command.

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

Syntax Description

detail	Displays detailed mDNS requests information.

name *record-name*	Displays detailed mDNS requests information based on name.
type *record-type*	Displays detailed mDNS requests information based on type.

Command Default

None

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

Example

This is an example of output from the **show mdns requests** command without any keywords:

```
Device# show mdns requests
MDNS Outstanding Requests
=====================================================
Request name  :   _airplay._tcp.local
Request type  :   PTR
Request class :   IN
-----------------------------------------------------
Request name  :   *.*
Request type  :   PTR
Request class :   IN
```

show mdns statistics

To display mDNS statistics for the device, use the **show mdns statistics** privileged EXEC command.

show mdns statistics {**all** | **service-list** *list-name* | **service-policy** {**all** | **interface** *type-number* }}

Syntax Description

all	Displays the service policy, service list, and interface information.
service-list *list-name*	Displays the service list information.
service-policy	Displays the service policy information.
interface *type number*	Displays interface information.

Command Default

None

Command Modes

Privileged EXEC

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

Example

This is an example of output from the **show mdns statistics all** command:

```
Device# show mdns statistics all
 mDNS Statistics
 mDNS packets sent       : 0
 mDNS packets received   : 0
 mDNS packets dropped    : 0
 mDNS cache memory in use: 64224(bytes)
```

show platform ip multicast

To display platform-dependent IP multicast tables and other information, use the **show platform ip multicast** privileged EXEC command.

show platform ip multicast {**groups** | **hardware [detail]** | **interfaces** | **retry**}

Syntax Description

groups	Displays IP multicast routes per group.
hardware [**detail**]	Displays IP multicast routes loaded into hardware. The optional **detail** keyword is used to show port members in the destination index and route index.
interfaces	Displays IP multicast interfaces.
retry	Displays the IP multicast routes in the retry queue.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is not supported on switches running the LAN Base feature set.

This example shows how to display platform IP multicast routes per group:

```
Device# show platform ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6  flags:  C
No RPF interface.
Number of OIF: 0
Flags: 0x10   Pkts : 0
OIF Details:No OIF interface.

DI details
----------
Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f6  index1:0x51f6

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
---------------------------------------

al_rsc_di
RM:index = 0x51f6
```

```
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f6
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==============================================================

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f6
RM:fd const lbl = 0x0
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1

==============================================================

HTM details
-----------
Handle:0x5d604490 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x5d604518  handle1:0x5d604580


Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604518)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x5d604580)

KEY - grp_addr:224.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:240.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 4095 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
```

```
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 164
capwap_mgid_present: 0 mgid 0

==============================================================


MROUTE ENTRY vrf 0 (*, 224.0.1.40)
Token: 0x0000001f8  flags:  C IC
RPF interface: Vl121(74238750229529173)): SVI
Token:0x00000021  flags: F IC NS
Number of OIF: 1
Flags: 0x10   Pkts : 0
OIF Details:
     Vl121      F IC NS
DI details
----------
Handle:0x603d0000 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f7  index1:0x51f7

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xe0 0x0 0x1 0x28 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
----------------------------------------

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

al_rsc_di
RM:index = 0x51f7
RM:pmap = 0x0
RM:cmi = 0x33f
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f7
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
```

```
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==============================================================

RI details
----------

SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f7
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x1
RM:remote data = 0x1

==============================================================

HTM details
-----------
Handle:0x603d0440 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x603cfae0  sm handle 0:0x603d0590  handle1:0x603d0520
sm handle 1:0x603d1770


Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603cfae0)

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x603d0520)

KEY - grp_addr:224.0.1.40 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 6 station_index: 165
capwap_mgid_present: 0 mgid 0

==============================================================


MROUTE ENTRY vrf 0 (*, 239.255.255.250)
Token: 0x0000003b7d  flags:  C
No RPF interface.
Number of OIF: 1
Flags: 0x10   Pkts : 95
OIF Details:
     Vl131      F NS
DI details
----------
```

```
Handle:0x606ffba0 Res-Type:ASIC_RSC_DI Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
Hardware Indices/Handles: index0:0x51f8  index1:0x51f8

Cookie length 56
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x20 0xef 0xff 0xff 0xfa 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0
0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)
----------------------------------------

al_rsc_di
RM:index = 0x51f8
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x0
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

al_rsc_di
RM:index = 0x51f8
RM:pmap = 0x0
RM:cmi = 0x0
RM:rcp_pmap = 0x1
RM:force data copy = 0
RM:remote cpu copy = 0
RM:remote data copy = 0
RM:local cpu copy = 0
RM:local data copy = 0

al_rsc_cmi
RM:index = 0x51f8
RM:cti_lo[0] = 0x0
RM:cti_lo[1] = 0x0
RM:cti_lo[2] = 0x0
RM:cpu_q_vpn[0] = 0x0
RM:cpu_q_vpn[1] = 0x0
RM:cpu_q_vpn[2] = 0x0
RM:npu_index = 0x0
RM:strip_seg = 0x0
RM:copy_seg = 0x0

==============================================================

RI details
----------

ASIC# 0
Replication list :
------------------

Total #ri : 0
start_ri : 15
common_ret : 0
```

```
ASIC# 1
Replication list :
------------------

Total #ri : 6
start_ri : 15
common_ret : 0

Replication entry rep_ri 0xF #elem = 1
0) ri[0]=50 port=58 dirty=0


ASIC# 2
Replication list :
------------------

Total #ri : 0
start_ri : 0
common_ret : 0


SI details
----------

RM:generic lbl = 0x0
RM:di_handle = 0x51f8
RM:fd const lbl = 0x8
RM:skipid_idx = 0x0
RM:rcp serviceid = 0x0
RM:dejavu prechken= 0x1
RM:local cpu = 0x0
RM:local data = 0x1
RM:remote cpu = 0x0
RM:remote data = 0x1

===============================================================

HTM details
-----------
Handle:0x606ff6f8 Res-Type:ASIC_RSC_STP_INDEX Asic-Num:255
Feature-ID:AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_ROUTE_STARG ref_count:1
Hardware Indices/Handles: handle0:0x606ff3e0  sm handle 0:0x60ab9160  handle1:0x606ff378
sm handle 1:0x60ab6cc0


Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff3e0)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0
Detailed Resource Information (ASIC# 1)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x606ff378)

KEY - grp_addr:239.255.255.250 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
MASK - grp_addr:0.0.0.0 decap_tunnel: 0 encap_tunnel: 0 vrf_id: 0 mtr_id: 0
AD: local_source_punt: 1 afd_label_or_clientid: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0

rpf_valid: 1 rpf_le_ptr: 0 afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1
cpp_type: 0 dest_mod_index: 0 rp_index: 0 priority: 3 rpf_le: 0 station_index: 178
capwap_mgid_present: 0 mgid 0
```

==========

wireless mdns-bridging

To enable Ethernet mDNS support, use the **wireless mdns-bridging** command. To disable Ethernet mDNS support, use the **no** form of this command.

wireless mdns-bridging

no wireless mdns-bridging

This command has no keywords or arguments.

Command Default

Ethernet mDNS support is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use this command only if you have enabled wireless multicast.

This example shows how to enable Ethernet mDNS support:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wireless mdns-bridging
```

wireless multicast

To enable Ethernet multicast support, use the **wireless multicast** command.

wireless multicast [**non-ip** [**vlan** *vlan-id*]]

Syntax Description

non-ip	(Optional) Configures multicast non-IP support.
vlan *vlan-id*	(Optional) Specifies multicast non-IP for a VLAN. The interface number ranges between 1 and 4095.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

This example shows how to configure multicast non-IP VLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast non-ip vlan 20
```

PART V

IPv6

- IPv6 Commands, page 267

CHAPTER 6

IPv6 Commands

- ipv6 flow monitor , page 267
- ipv6 traffic-filter , page 268
- show wireless ipv6 statistics , page 269

ipv6 flow monitor

This command activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.

To activate a previously created flow monitor, use the **ipv6 flow monitor** command. To de-activate a flow monitor, use the **no** form of the command.

ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

no ipv6 flow monitor *ipv6-monitor-name* [**sampler** *ipv6-sampler-name*] {**input**| **output**}

Syntax Description

ipv6-monitor-name	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
sampler *ipv6-sampler-name*	Applies the flow monitor sampler.
input	Applies the flow monitor on input traffic.
output	Applies the flow monitor on output traffic.

Command Default

IPv6 flow monitor is not activated until it is assigned to an interface.

Command Modes

Interface Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

```
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
Device(config-if)# end
```

ipv6 traffic-filter

This command enables IPv6 traffic filter.

To enable the filtering of IPv6 traffic on an interface, use the **ipv6 traffic-filter** command. To disable the filtering of IPv6 traffic on an interface, use the **no** form of the command.

Use the **ipv6 traffic-filter** interface configuration command on the switch stack or on a standalone switch to filter IPv6 traffic on an interface. The type and direction of traffic that you can filter depends on the feature set running on the switch stack. Use the **no** form of this command to disable the filtering of IPv6 traffic on an interface.

ipv6 traffic-filter [web] *acl-name*

no ipv6 traffic-filter [web]

Syntax Description

web	(Optional) Specifies an IPv6 access name for the WLAN Web ACL.
acl-name	Specifies an IPv6 access name.

Command Default

Filtering of IPv6 traffic on an interface is not configured.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To configure the dual IPv4 and IPv6 template, enter the **sdm prefer dual-ipv4-and-ipv6 {default | vlan}** global configuration command and reload the switch.

You can use the **ipv6 traffic-filter** command on physical interfaces (Layer 2 or Layer 3 ports), Layer 3 port channels, or switch virtual interfaces (SVIs).

You can apply an ACL to outbound or inbound traffic on Layer 3 interfaces (port ACLs), or to inbound traffic on Layer 2 interfaces (router ACLs).

If **any** port ACL (IPv4, IPv6, or MAC) is applied to an interface, that port ACL is used to filter packets, and any router ACLs attached to the SVI of the port VLAN are ignored.

This example shows how to filter IPv6 traffic on an interface:

```
Device(config-wlan)# ipv6 traffic-filter TestDocTrafficFilter
```

show wireless ipv6 statistics

This command is used to display the IPv6 packet counter statistics.

To view IPv6 packet counter statistics, use the **show wireless ipv6 statistics** command.

show wireless ipv6 statistics

Command Default

None.

Command Modes

User EXEC.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following example shows the summary of the IPv6 packet counter statistics:

```
Device# show wireless ipv6 statistics
NS Forwarding to wireless clients               : Enabled

RS count                                        : 0
RA count                                        : 0
NS count                                        : 0
NA count                                        : 0
Other NDP packet count                          : 0
----------------------------------------------------
Non-IPv6 packets count                          : 0
Non-IPv6 Multicast Destination MAC packet count : 0
Invalid length packets count                    : 0
Null packets count                              : 0
Invalid Source MAC packets count                : 0
----------------------------------------------------
TCP packets count                               : 0
UDP packets count                               : 0
Fragmented packets count                        : 0
```

```
No next header packets count                    : 0
Other type packets count                        : 0
----------------------------------------------------
Total packets count                             : 0
----------------------------------------------------
Blocked RA packets count                        : 0
Blocked NS packets count                        : 0
```

PART VI

Layer 2/3

- Layer 2/3 Commands, page 273

CHAPTER 7

Layer 2/3 Commands

- channel-group, page 274
- channel-protocol, page 277
- clear lacp, page 278
- clear pagp, page 279
- clear spanning-tree counters, page 279
- clear spanning-tree detected-protocols, page 280
- debug etherchannel, page 281
- debug lacp, page 282
- debug pagp, page 283
- debug platform pm, page 284
- debug platform udld, page 286
- debug spanning-tree , page 286
- interface port-channel, page 288
- lacp max-bundle, page 289
- lacp port-priority, page 290
- lacp rate, page 291
- lacp system-priority, page 292
- pagp learn-method, page 293
- pagp port-priority, page 294
- port-channel, page 295
- port-channel auto, page 295
- port-channel load-balance, page 296
- port-channel load-balance extended, page 297
- port-channel min-links, page 299

- rep admin vlan, page 300
- rep block port, page 300
- rep lsl-age-timer, page 302
- rep lsl-retries, page 302
- rep preempt delay, page 303
- rep preempt segment, page 304
- rep segment, page 305
- rep stcn, page 306
- show etherchannel, page 307
- show interfaces rep detail, page 309
- show lacp, page 310
- show pagp, page 314
- show platform etherchannel, page 315
- show platform pm, page 316
- show rep topology, page 317
- show udld, page 318
- switchport, page 322
- switchport access vlan, page 323
- switchport mode, page 324
- switchport nonegotiate, page 326
- switchport voice vlan, page 327
- udld, page 329
- udld port, page 330
- udld reset, page 332

channel-group

To assign an Ethernet port to an EtherChannel group, or to enable an EtherChannel mode, or both, use the **channel-group** command in interface configuration mode. To remove an Ethernet port from an EtherChannel group, use the **no** form of this command.

channel-group *channel-group-number* **mode** {**active**| **auto** [**non-silent**]| **desirable** [**non-silent**]| **on**| **passive**}

no channel-group

Syntax Description

channel-group-number	Channel group number. The range is 1 to 128.

mode	Specifies the EtherChannel mode.
active	Unconditionally enables Link Aggregation Control Protocol (LACP).
auto	Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.
non-silent	(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device.
desirable	Unconditionally enables PAgP.
on	Enables the on mode.
passive	Enables LACP only if a LACP device is detected.

Command Default

No channel groups are assigned.

No mode is configured.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, the **channel-group** command automatically creates the port-channel interface when the channel group gets its first physical port. You do not have to use the **interface port-channel** command in global configuration mode to manually create a port-channel interface. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.

Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When desirable is enabled, silent operation is the default.

If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the device is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.

Caution Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same device or on different devices in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Caution Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

This example shows how to configure an EtherChannel on a single device in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode desirable
Device(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single device in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/1 -2
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode active
Device(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel in a device stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

```
Device# configure terminal
Device(config)# interface range gigabitethernet2/0/4 -5
Device(config-if-range)# switchport mode access
Device(config-if-range)# switchport access vlan 10
Device(config-if-range)# channel-group 5 mode passive
Device(config-if-range)# exit
Device(config)# interface gigabitethernet3/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 10
Device(config-if)# channel-group 5 mode passive
Device(config-if)# exit
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

channel-protocol {**lacp**| **pagp**}

no channel-protocol

Syntax Description

lacp	Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).
pagp	Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You cannot configure PAgP on cross-stack configurations.

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Device(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [*channel-group-number*] **counters**

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

This example shows how to clear all channel-group information:

```
Device# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Device# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp** *channel-group-number* **counters** privileged EXEC command.

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp [*channel-group-number*] **counters**

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Clears traffic counters.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

This example shows how to clear all channel-group information:

```
Device# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Device# clear pagp 10 counters
```

You can verify that the information was deleted by entering the **show pagp** privileged EXEC command.

clear spanning-tree counters

To clear the spanning-tree counters, use the **clear spanning-tree counters** command in privileged EXEC mode.

clear spanning-tree counters [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Clears all spanning-tree counters on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 128.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the *interface-id* value is not specified, spanning-tree counters are cleared for all interfaces.

This example shows how to clear spanning-tree counters for all interfaces:

```
Device# clear spanning-tree counters
```

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring devices on the interface, use the **clear spanning-tree detected-protocols** command in privileged EXEC mode.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 128.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A device running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D devices. If a rapid-PVST+ or an MSTP device receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the device sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) device can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

The device does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

This example shows how to restart the protocol migration process on a port:

```
Device# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

debug etherchannel

To enable debugging of EtherChannels, use the **debug etherchannel** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

no debug etherchannel [**all** | **detail** | **error** | **event** | **idb**]

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

Note Although the **linecard** keyword is displayed in the command-line help, it is not supported.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all EtherChannel debug messages:

```
Device# debug etherchannel all
```

This example shows how to display debug messages related to EtherChannel events:

```
Device# debug etherchannel event
```

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

no debug lacp [**all** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays messages about changes within the LACP finite state machine.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays the receiving and transmitting LACP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all LACP debug messages:

```
Device# debug LACP all
```

This example shows how to display debug messages related to LACP events:

```
Device# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

no debug pagp [**all** | **dual-active** | **event** | **fsm** | **misc** | **packet**]

Syntax Description

all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays dual-active detection messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
misc	(Optional) Displays miscellaneous PAgP debug messages.

packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug pagp** command is the same as the **no debug pagp** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all PAgP debug messages:

```
Device# debug pagp all
```

This example shows how to display debug messages related to PAgP events:

```
Device# debug pagp event
```

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

no debug platform pm {**all**| **counters**| **errdisable**| **fec**| **if-numbers**| **l2-control**| **link-status**| **platform**| **pm-spi**| **pm-vectors [detail]**| **ses**| **vlans**}

Syntax Description

all	Displays all port manager debug messages.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.

fec	Displays forwarding equivalence class (FEC) platform-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
l2-control	Displays Layer 2 control infra debug messages.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-spi	Displays port manager stateful packet inspection (SPI) event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.
detail	(Optional) Displays vector-function details.
ses	Displays service expansion shelf (SES) related event debug messages.
vlans	Displays VLAN creation and deletion event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform pm** command is the same as the **no debug platform pm** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Device# debug platform pm vlans
```

debug platform udld

To enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software, use the **debug platform udld** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform udld [**error**| **event**] [**switch** *switch-number*]

no debug platform udld [**error**| **event**] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays error condition debug messages.
event	(Optional) Displays UDLD-related platform event debug messages.
switch *switch-number*	(Optional) Displays UDLD debug messages for the specified stack member.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform udld** command is the same as the **no debug platform udld** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session** *switch-number* EXEC command. Then enter the **debug** command at the command-line prompt of the stack member.

debug spanning-tree

To enable debugging of spanning-tree activities, use the **debug spanning-tree** command in EXEC mode. To disable debugging, use the **no** form of this command.

debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **ha** | **mstp** | **pvst+**| **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}

no debug spanning-tree {**all** | **backbonefast** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+**| **root** | **snmp** | **synchronization** | **switch** | **uplinkfast**}

Syntax Description

all	Displays all spanning-tree debug messages.
backbonefast	Displays BackboneFast-event debug messages.
bpdu	Displays spanning-tree bridge protocol data unit (BPDU) debug messages.
bpdu-opt	Displays optimized BPDU handling debug messages.
config	Displays spanning-tree configuration change debug messages.
etherchannel	Displays EtherChannel-support debug messages.
events	Displays spanning-tree topology event debug messages.
exceptions	Displays spanning-tree exception debug messages.
general	Displays general spanning-tree activity debug messages.
ha	Displays high-availability spanning-tree debug messages.
mstp	Debugs Multiple Spanning Tree Protocol (MSTP) events.
pvst+	Displays per-VLAN spanning-tree plus (PVST+) event debug messages.
root	Displays spanning-tree root-event debug messages.
snmp	Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.
switch	Displays device shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms.
synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug spanning-tree** command is the same as the **no debug spanning-tree** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch , start a session from the active switch by using the **session** *switch-number* command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display all spanning-tree debug messages:

```
Device# debug spanning-tree all
```

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

interface port-channel *port-channel-number*

no interface port-channel

Syntax Description

port-channel-number	Channel group number. The range is 1 to 128.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** interface configuration command, which automatically creates the port-channel interface when the channel group obtains its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*,

or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Only one port channel in a channel group is allowed.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical port and not on the port channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

This example shows how to create a port channel interface with a port channel number of 5:

```
Device(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

lacp max-bundle

To define the maximum number of active LACP ports allowed in a port channel, use the **lacp max-bundle** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp max-bundle *max_bundle_number*

no lacp max-bundle

Syntax Description

max_bundle_number	The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in hot-standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled

into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **lacp max-bundle** command must specify a number greater than the number specified by the **port-channel min-links** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a maximum of five active LACP ports in port channel 2:

```
Device(config)# interface port-channel 2
Device(config-if)# lacp max-bundle 5
```

lacp port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lacp port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lacp port-priority *priority*

no lacp port-priority

Syntax Description

priority	Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically lower value has a higher priority: When there are more than eight ports in an LACP channel group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), then an internal value for the port number determines the priority.

Note The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the **lacp system-priority** global configuration command for determining which device controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the configuration guide for this release.

This example shows how to configure the LACP port priority on a port:

```
Device# interface gigabitethernet2/0/1
Device(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

lacp rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the **lacp rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command

lacp rate {**normal** | **fast**}

no lacp rate

Syntax Description

normal	Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.
fast	Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

Command Default

The default ingress rate for control packets is 30 seconds after the link is bundled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines

Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate configured on the interface. Using the **lacp rate**command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.

This command is supported only on LACP-enabled interfaces.

This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:

```
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lacp rate fast
```

lacp system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lacp system-priority** command in global configuration mode on the device. To return to the default setting, use the **no** form of this command.

lacp system-priority *priority*

no lacp system-priority

Syntax Description

priority	System priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **lacp system-priority** command determines which device in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have a higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the device MAC address) determines which device is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the device.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to set the LACP system priority:

```
Device(config)# lacp system-priority 20000
```

You can verify your settings by entering the **show lacp sys-id** privileged EXEC command.

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

pagp learn-method {**aggregation-port**| **physical-port**}

no pagp learn-method

Syntax Description

aggregation-port	Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.
physical-port	Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

Command Default

The default is aggregation-port (logical port channel).

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The learn method must be configured the same at both ends of the link.

The device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the

port-channel load-balance src-mac global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Device(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port channel within the EtherChannel:

```
Device(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*

no pagp port-priority

Syntax Description

priority	Priority number. The range is from 0 to 255.

Command Default

The default is 128.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The physical port with the highest priority that is operational and has membership in the same EtherChannel is the one selected for PAgP transmission.

The device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

This example shows how to set the port priority to 200:

```
Device(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

port-channel

To convert the auto created EtherChannel into a manual channel and adding configuration on the EtherChannel, use the **port-channel** command in privileged EXEC mode.

port-channel {*channel-group-number* **persistent** | **persistent** }

Syntax Description

channel-group-number	Channel group number. The range is 1 to 128.
persistent	Converts the auto created EtherChannel into a manual channel and allows you to add configuration on the EtherChannel.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.2E	This command was introduced.

Usage Guidelines

You can use the **show etherchannel summary** privileged EXEC command to display the EtherChannel information.

This example shows how to convert the auto created EtherChannel into a manual channel:

```
Device# port-channel 1 persistent
```

port-channel auto

To enable the auto-LAG feature on a switch globally, use the **port-channel auto** command in global configuration mode. To disable the auto-LAG feature on the switch globally, use **no** form of this command.

port-channel auto

no port-channel auto

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the auto-LAG feature is disabled globally and is enabled on all port interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.7.2E	This command was introduced.

Usage Guidelines

You can use the **show etherchannel auto** privileged EXEC command to verify if the EtherChannel was created automatically.

This example shows how to enable the auto-LAG feature on the switch:

```
Device(config)# port-channel auto
```

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load-balancing mechanism to the default setting, use the **no** form of this command.

port-channel load-balance {**dst-ip**| **dst-mac**| **dst-mixed-ip-port**| **dst-port**| **extended**| **src-dst-ip**| **src-dst-mac**| **src-dst-mixed-ip-port**| **src-dst-port**| **src-ip**| **src-mac**| **src-mixed-ip-port**| **src-port**}

no port-channel load-balance

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-mixed-ip-port	Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.
dst-port	Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.

extended	Sets extended load balance methods among the ports in the EtherChannel. See the **port-channel load-balance extended** command.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-dst-mixed-ip-port	Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.
src-dst-port	Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-mixed-ip-port	Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.
src-port	Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

This example shows how to set the load-distribution method to dst-mac:

```
Device(config)# port-channel load-balance dst-mac
```

port-channel load-balance extended

To set combinations of load-distribution methods among the ports in the EtherChannel, use the **port-channel load-balance extended** command in global configuration mode. To reset the extended load-balancing mechanism to the default setting, use the **no** form of this command.

port-channel load-balance extended[**dst-ip**| **dst-mac**| **dst-port**| **ipv6-label**| **l3-proto**| **src-ip**| **src-mac**| **src-port**]

no port-channel load-balance extended

Syntax Description

dst-ip	(Optional) Specifies load distribution based on the destination host IP address.
dst-mac	(Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-port	(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
ipv6-label	(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.
l3-proto	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.
src-ip	(Optional) Specifies load distribution based on the source host IP address.
src-mac	(Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-port	(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For information about when to use these forwarding methods, see the *Layer 2/3 Configuration Guide (Catalyst 3850 Switches)* for this release.

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

This example shows how to set the extended load-distribution method:

```
Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

To define the minimum number of LACP ports that must be bundled in the link-up state and bundled in the EtherChannel in order that a port channel becomes active, use the **port-channel min-links** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

port-channel min-links *min_links_number*

no port-channel min-links

Syntax Description

min_links_number	The minimum number of active LACP ports in the port channel. The range is 2 to 8. The default is 1.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in hot-standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **port-channel min-links** command must specify a number a less than the number specified by the **lacp max-bundle** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:

```
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
```

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

rep admin vlan *vlan-id*

no rep admin vlan

Syntax Description

vlan-id	The 48-bit static MAC address.

Command Default

The default value of the administrative VLAN is VLAN 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

The range of the REP administrative VLAN is from 2 to 4094.

If you do not configure an administrative VLAN, the default VLAN is VLAN 1. The default VLAN 1 is always configured. There can be only one administrative VLAN on a router and on a segment.

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Device(config)#  rep admin vlan 100
```

rep block port

To configure a REP VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

rep block port {**id** *port-id* | *neighbor-offset* | **preferred**} **vlan** {*vlan-list* | **all**}

no rep block port {**id** *port-id* | *neighbor-offset* | **preferred**}

Syntax Description

id *port-id*	Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can display the port ID for an interface by entering the **show interface** *interface-id* **rep detail** command in privileged EXEC mode.
neighbor-offset	Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is from -256 to +256; a value of 0 is invalid.
preferred	Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
vlan	Identifies the VLANs to be blocked.
vlan-list	VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) to be blocked.
all	Blocks all the VLANs.

Command Default

The default behavior after you enter the **rep preempt segment** command in privileged EXEC (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. Do not enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** command in interface configuration mode and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. To determine the port ID of a port, enter the **show interfaces** *interface-id* **rep detail** command in privileged EXEC mode.

The following example shows how to configure REP VLAN load balancing.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep block port id 0009001818D68700 vlan 1-100
```

rep lsl-age-timer

To configure the REP link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

rep lsl-age-timer *milliseconds*

no rep lsl-age-timer *milliseconds*

Syntax Description

milliseconds	REP LSL age-out timer value in milliseconds (ms). The range is from 120 ms to 10000 ms in multiples of 40 ms.

Command Default

The default LSL age-out timer value is 5 ms.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

The **rep lsl-age-timer** command is used to configure the REP LSL age-out timer value. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL age-out timer value.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 1 edge primary
Device(config-if)#  rep lsl-age-timer 2000
```

rep lsl-retries

To configure the REP link status layer (LSL) number of retries, use the **rep lsl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

rep lsl-retries *number-of-retries*

no rep lsl-retries *number-of-retries*

Syntax Description

number-of-retries	Number of LSL retries. The range of retries is from 3 to 10.

Command Default

The default number of LSL retries is 5.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL retries.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 2 edge primary
```

rep preempt delay

To configure a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*

no rep preempt delay

Syntax Description

seconds	Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.

Command Default

REP preemption delay is not set. The default is manual preemption without delay.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

You can verify your settings by entering the **show interfaces rep** privileged EXEC command.

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep preempt delay 100
```

rep preempt segment

To manually start REP VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

rep preempt segment *segment-id*

Syntax Description

segment-id	ID of the REP segment. The range is from 1 to 1024.

Command Default

Manual preemption is the default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the router.

Ensure that all the other segment configuration is completed before setting preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not enter the **rep preempt delay** *seconds* command in interface configuration mode on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior-the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** command in interface configuration mode on the REP primary edge port before you manually start preemption.

The following example shows how to manually trigger REP preemption on segment 100.

```
Device#  rep preempt segment 100
```

rep segment

To enable REP on the interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

Syntax Description

segment-id	Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Configures the port as an edge port. Each segment has only two edge ports.
no-neighbor	(Optional) Specifies the segment edge as one with no external REP neighbor.
primary	(Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port.
preferred	(Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing. **Note** Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Command Default

REP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port.

If REP is enabled on two ports on a router, both ports must be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a router is configured in a segment, the port should be an edge port.
- If two ports on a router belong to the same segment, both ports must be regular segment ports.
- If two ports on a router belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. Be aware of this to avoid sudden connection losses.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

The following example shows how to enable REP on a regular (nonedge) segment port.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#  rep segment 1 edge no-neighbor primary
```

rep stcn

To configure a REP edge port to send segment topology change notifications (STCNs) to another interface or to other segments, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface or to the segment, use the **no** form of this command.

rep stcn {**interface** *interface-id* | **segment** *segment-id-list*}

no rep stcn {**interface** | **segment**}

Syntax Description

interface *interface-id*	Specifies a physical interface or port channel to receive STCNs.
segment *segment-id-list*	Specifies one REP segment or a list of segments to receive STCNs. The segment range is from 1 to 1024. You can also configure a sequence of segments (for example 3 to 5, 77, 100).

Command Default

Transmission of STCNs to other interfaces or segments is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50.

```
Device(config)#  interface TenGigabitEthernet 4/1
Device(config-if)#   rep stcn segment 25-50
```

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

show etherchannel [*channel-group-number* | {**detail | port | port-channel | protocol | summary** }] | [**detail| load-balance | port| port-channel| protocol| summary**]

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
detail	(Optional) Displays detailed EtherChannel information.
load-balance	(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.
port	(Optional) Displays EtherChannel port information.
port-channel	(Optional) Displays port-channel information.

protocol	(Optional) Displays the protocol that is being used in the channel.
summary	(Optional) Displays a one-line summary per channel group.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not specify a channel group number, all channel groups are displayed.

This is an example of output from the **show etherchannel** *channel-group-number* **detail** command:

```
Device> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                  Ports in the group:
                  -------------------
Port: Gi1/0/1
------------
Port state    = Up Mstr In-Bndl
Channel group = 1        Mode  = Active        Gcchange = -
Port-channel  =          Po1GC = -             Pseudo port-channel = Po1
Port index    =          0Load = 0x00          Protocol = LACP

Flags: S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
       A - Device is in active mode.        P - Device is in passive mode.

Local information:
                         LACP port   Admin   Oper   Port   Port
Port     Flags   State   Priority    Key     Key    Number State
Gi1/0/1   SA      bndl     32768      0x1     0x1    0x101  0x3D
Gi1/0/2    A      bndl     32768      0x0     0x1    0x0    0x3D

Age of the port in the current state: 01d:20h:06m:04s

                   Port-channels in the group:
                   ----------------------

Port-channel: Po1   (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1          Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load   Port      EC state        No of bits
------+------+------+------------------+-----------
```

```
 0      00    Gi1/0/1    Active           0
 0      00    Gi1/0/2    Active           0

Time since last port bundled:   01d:20h:24m:44s   Gi1/0/2
```

This is an example of output from the **show etherchannel** *channel-group-number* **summary** command:

```
Device> show etherchannel 1 summary
Flags: D - down P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3 S - Layer2
       u - unsuitable for bundling
       U - in use f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------------------
 1     Po1(SU)       LACP        Gi1/0/1(P) Gi1/0/2(P)
```

This is an example of output from the **show etherchannel** *channel-group-number* **port-channel** command:

```
Device> show etherchannel 1 port-channel
Port-channels in the group:
----------------------
Port-channel: Po1 (Primary Aggregator)
------------
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load   Port   EC state           No of bits
------+------+------+------------------+-----------
 0      00    Gi1/0/1 Active             0
 0      00    Gi1/0/2 Active             0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Device# show etherchannel protocol
Channel-group listing:
----------------------
Group: 1
----------
Protocol: LACP
Group: 2
----------
Protocol: PAgP
```

show interfaces rep detail

To display detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

show interfaces [*interface-id*] **rep detail**

Syntax Description

interface-id	(Optional) Physical interface used to display the port ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to display the REP configuration and status for a specified interface.

```
Device#  show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

show lacp [*channel-group-number*] {**counters**| **internal**| **neighbor**| **sys-id**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Displays traffic information.
internal	Displays internal information.
neighbor	Displays neighbor information.

sys-id	Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* to specify a channel group for all keywords except **sys-id**.

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Device> show lacp counters
              LACPDUs        Marker     Marker Response   LACPDUs
Port        Sent  Recv     Sent  Recv     Sent  Recv     Pkts  Err
---------------------------------------------------------------------
Channel group:1
Gi2/0/1      19    10        0    0         0    0        0
Gi2/0/2      14    6         0    0         0    0        0
```

Table 19: show lacp counters Field Descriptions

Field	Description
LACPDUs Sent and Recv	The number of LACP packets sent and received by a port.
Marker Sent and Recv	The number of LACP marker packets sent and received by a port.
Marker Response Sent and Recv	The number of LACP marker response packets sent and received by a port.
LACPDUs Pkts and Err	The number of unknown and illegal packets received by LACP for a port.

This is an example of output from the **show lacp internal** command:

```
Device> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port    Admin    Oper    Port     Port
Port      Flags   State     Priority     Key      Key     Number   State
Gi2/0/1    SA      bndl      32768         0x3     0x3       0x4    0x3D
Gi2/0/2    SA      bndl      32768         0x3     0x3       0x5    0x3D
```

The following table describes the fields in the display:

Table 20: show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: • **– —**Port is in an unknown state. • **bndl—**Port is attached to an aggregator and bundled with other ports. • **susp—**Port is in a suspended state; it is not attached to any aggregator. • **hot-sby—**Port is in a hot-standby state. • **indiv—**Port is incapable of bundling with any other port. • **indep—**Port is in an independent state (not bundled but able to handle data traffic. In this case, LACP is not running on the partner port). • **down—**Port is down.
LACP Port Priority	Port priority setting. LACP uses the port priority to put ports in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
Admin Key	Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish.

Field	Description
Oper Key	Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number.
Port Number	Port number.
Port State	State variables for the port, encoded as individual bits within a single octet with these meanings: • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired **Note** In the list above, bit7 is the MSB and bit0 is the LSB.

This is an example of output from the **show lacp neighbor** command:

```
Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
       A - Device is in Active mode        P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner                Partner                Partner
Port      System ID              Port Number   Age      Flags
Gi2/0/1   32768,0007.eb49.5e80   0xC             19s     SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C

Partner's information:

          Partner                Partner                Partner
Port      System ID              Port Number   Age      Flags
Gi2/0/2   32768,0007.eb49.5e80   0xD             15s     SP

          LACP Partner           Partner       Partner
          Port Priority          Oper Key      Port State
          32768                  0x3           0x3C
```

This is an example of output from the **show lacp sys-id** command:

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

show pagp [*channel-group-number*] {**counters**| **dual-active**| **internal**| **neighbor**}

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Displays traffic information.
dual-active	Displays the dual-active status.
internal	Displays internal information.
neighbor	Displays neighbor information.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

This is an example of output from the **show pagp 1 counters** command:

```
Device> show pagp 1 counters
             Information        Flush
Port         Sent   Recv     Sent   Recv
----------------------------------------
Channel group: 1
  Gi1/0/1    45     42       0      0
  Gi1/0/2    45     41       0      0
```

This is an example of output from the **show pagp dual-active** command:

```
Device> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
          Dual-Active     Partner              Partner   Partner
Port      Detect Capable  Name                 Port      Version
Gi1/0/1   No              Device               Gi3/0/3   N/A
Gi1/0/2   No              Device               Gi3/0/4   N/A

<output truncated>
```

This is an example of output from the **show pagp 1 internal** command:

```
Device> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi1/0/1     SC    U6/S7   H       30s      1        128        Any      16
Gi1/0/2     SC    U6/S7   H       30s      1        128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Device> show pagp 1 neighbor

Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.        P - Device learns on physical port.

Channel group 1 neighbors
            Partner              Partner          Partner           Partner Group
Port        Name                 Device ID        Port         Age  Flags   Cap.
Gi1/0/1     device-p2            0002.4b29.4600   Gi01//1        9s SC      10001
Gi1/0/2     device-p2            0002.4b29.4600   Gi1/0/2       24s SC      10001
```

show platform etherchannel

To display platform-dependent EtherChannel information, use the **show platform etherchannel** command in privileged EXEC mode.

show platform etherchannel *channel-group-number* {**group-mask**| **load-balance mac** *src-mac dst-mac* [**ip** *src-ip dst-ip* [**port** *src-port dst-port*]]} [**switch** *switch-number*]

Syntax Description

channel-group-number	Channel group number. The range is 1 to 128.
group-mask	Displays EtherChannel group mask.
load-balance	Tests EtherChannel load-balance hash algorithm.
mac *src-mac dst-mac*	Specifies the source and destination MAC addresses.
ip *src-ip dst-ip*	(Optional) Specifies the source and destination IP addresses.

port *src-port dst-port*	(Optional) Specifies the source and destination layer port numbers.
switch *switch-number*	(Optional) Specifies the stack member.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Do not use this command unless a technical support representative asks you to do so.

show platform pm

To display platform-dependent port manager information, use the **show platform pm** command in privileged EXEC mode.

show platform pm {**etherchannel** *channel-group-number* **group-mask**| **interface-numbers**| **port-data** *interface-id*| **port-state**| **spi-info**| **spi-req-q**}

Syntax Description

etherchannel *channel-group-number* **group-mask**	Displays the EtherChannel group-mask table for the specified channel group. The range is 1 to 128.
interface-numbers	Displays interface numbers information.
port-data *interface-id*	Displays port data information for the specified interface.
port-state	Displays port state information.
spi-info	Displays stateful packet inspection (SPI) information.
spi-req-q	Displays stateful packet inspection (SPI) maximum wait time for acknowledgment.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Use this command only when you are working directly with your technical support representative while troubleshooting a problem.

Do not use this command unless your technical support representative asks you to do so.

show rep topology

To display REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description

segment *segment-id*	(Optional) Specifies the segment for which to display REP topology information. The ID range is from 1 to 1024.
archive	(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.
detail	(Optional) Displays detailed REP topology information.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced

The following is sample output from the show rep topology command.

```
Device#  show rep topology

REP Segment 1
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Te5/4      Pri  Open
10.64.106.228    Te3/4           Open
10.64.106.228    Te3/3           Open
10.64.106.67     Te4/3           Open
10.64.106.67     Te4/4           Alt
10.64.106.63     Te4/4      Sec  Open

REP Segment 3
BridgeName       PortName   Edge Role
---------------- ---------- ---- ----
10.64.106.63     Gi50/1     Pri  Open
SVT_3400_2       Gi0/3           Open
SVT_3400_2       Gi0/4           Open
10.64.106.68     Gi40/2          Open
10.64.106.68     Gi40/1          Open
10.64.106.63     Gi50/2     Sec  Alt
```

The following is sample output from the **show rep topology detail** command.

```
Device#  show rep topology detail

REP Segment 1
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

show udld

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show udld** command in user EXEC mode.

show udld [**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**] *interface_number*

show udld neighbors

Syntax Description

Auto-Template	(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.
Capwap	(Optional) Displays UDLD operational status of the CAPWAP interface. The range is from 0 to 2147483647.
GigabitEthernet	(Optional) Displays UDLD operational status of the GigabitEthernet interface. The range is from 0 to 9.
GroupVI	(Optional) Displays UDLD operational status of the group virtual interface. The range is from 1 to 255.
InternalInterface	(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.
Loopback	(Optional) Displays UDLD operational status of the loopback interface. The range is from 0 to 2147483647.
Null	(Optional) Displays UDLD operational status of the null interface.
Port-channel	(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is from 1 to 128.
TenGigabitEthernet	(Optional) Displays UDLD operational status of the Ten Gigabit Ethernet interface. The range is from 0 to 9.
Tunnel	(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.
Vlan	(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.
interface-id	(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.
neighbors	(Optional) Displays neighbor information only.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The table that follows describes the fields in this display.

```
Device> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 21: show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.

Field	Description
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udld neighbors** command:

```
Device# show udld neighbors
Port     Device Name          Device ID  Port-ID  OperState
```

```
-------- -------------------- ---------- -------- --------------
Gi2/0/1  Switch-A             1          Gi2/0/1  Bidirectional
Gi3/0/1  Switch-A             2          Gi3/0/1  Bidirectional
```

switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

switchport

no switchport

Syntax Description

This command has no arguments or keywords.

Command Default

By default, all interfaces are in Layer 2 mode.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.

Note This command is not supported on devices running the LAN Base feature set.

Entering the **no switchport** command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.

Note If an interface is configured as a Layer 3 interface, you must first enter the **switchport** command to configure the interface as a Layer 2 port. Then you can enter the **switchport access vlan** and **switchport mode** commands.

The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the port status of an interface by entering the **show running-config** privileged EXEC command.

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Device(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode for the device, use the **no** form of this command.

switchport access vlan *vlan-id*

no switchport access vlan

Syntax Description

vlan-id	VLAN ID of the access mode VLAN; the range is 1 to 4094.

Command Default

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The port must be in access mode before the **switchport access vlan** command can take effect.

If the switchport mode is set to **access vlan** *vlan-id*, the port operates as a member of the specified VLAN. An access port can be assigned to only one VLAN.

The **no switchport access** command resets the access mode VLAN to the appropriate default VLAN for the device.

This example shows how to change a switched port interface that is operating in access mode to operate in VLAN 2 instead of the default VLAN:

```
Device(config-if)# switchport access vlan 2
```

switchport mode

To configure the VLAN membership mode of a port, use the **switchport mode** command in interface configuration mode. To reset the mode to the appropriate default for the device, use the **no** form of this command.

switchport mode {**access**| **dynamic** | {**auto**| **desirable**}| **trunk**}

noswitchport mode {**access**| **dynamic** | {**auto**| **desirable**}| **trunk**}

Syntax Description

access	Sets the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives nonencapsulated (non-tagged) frames. An access port can be assigned to only one VLAN.
dynamic auto	Sets the port trunking mode dynamic parameter to auto to specify that the interface convert the link to a trunk link. This is the default switchport mode.
dynamic desirable	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.
trunk	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two devices or between a device and a router.

Command Default

The default mode is **dynamic auto**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A configuration that uses the **access**,or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.

To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this problem, configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

Access ports and trunk ports are mutually exclusive.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a port set to **dynamic auto** or **dynamic desirable**, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to **dynamic auto** or **dynamic desirable**, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the *Administrative Mode* and *Operational Mode* rows.

This example shows how to configure a port for access mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode trunk
```

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

switchport nonegotiate

no switchport nonegotiate

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no switchport nonegotiate** command removes nonegotiate status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk.**

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name** *vlan_name*}

no switchport voice vlan

Syntax Description

vlan-id	The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
dot1p	Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none	Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged	Configures the telephone to send untagged voice traffic. This is the default for the telephone.
vlan *vlan_name*	(Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default

The default is not to automatically configure the telephone (**none**).

The telephone default is not to tag frames.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
15.2(4)E	Option to specify a VLAN name for access and voice VLAN. The "**name**" keyword was added.

Usage Guidelines

You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the device to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the interface by entering the **trust device cisco-phone** interface configuration command. If you use the auto QoS feature, these settings are automatically configured.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The device puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1p**, **none**, or **untagged**, the device puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces** *interface-id* **switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database:

```
Device# show vlan id 55
VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
55 test active
VLAN Type  SAID   MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- ------ ---- -----  ------ -------- --- -------- ------ ------
55   enet  100055 1500 -      -      -        -   -        0      0
Remote SPAN VLAN
----------------
Disabled
Primary Secondary Type Ports
------- --------- ----------------- ------------------------------------------
```

Part 3- Setting the VLAN on the interface, by using the vlan_name 'test':

```
Device# configure terminal
Device(config)# interface gigabitethernet5/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

Part 4 - Verifying running-config:

```
Device# show running-config
interface gigabitethernet5/1
Building configuration...
Current configuration : 113 bytes
```

```
!
interface GigabitEthernet5/1
switchport voice vlan 55
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport:

```
Device# show interface GigabitEthernet5/1 switchport
Name: Gi5/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#
```

udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

udld {**aggressive**| **enable**| **message time** *message-timer-interval*}

no udld {**aggressive**| **enable**| **message**}

Syntax Description

aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
enable	Enables UDLD in normal mode on all fiber-optic interfaces.
message time *message-timer-interval*	Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 1 to 90 seconds. The default is 15 seconds.

Command Default

UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the *Catalyst 2960-X Switch Layer 2 Configuration GuideCatalyst 2960-XR Switch Layer 2 Configuration GuideLayer 2/3 Configuration Guide (Catalyst 3850 Switches)*.

If you change the message time between probe packets, you are making a compromise between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command followed by the **udld {aggressive | enable}** global configuration command to reenable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenable UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Device(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC command.

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [aggressive]

no udld port [aggressive]

Syntax Description

aggressive	(Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

This example shows how to reset all interfaces disabled by UDLD:

```
Device# udld reset
1 ports shutdown by UDLD were reset.
```

PART VII

Lightweight Access Point

- Cisco Lightweight Access Point Commands, page 335

CHAPTER 8

Cisco Lightweight Access Point Commands

- ap auth-list ap-policy, page 341
- ap bridging, page 341
- ap capwap multicast, page 342
- ap capwap retransmit, page 343
- ap capwap timers, page 344
- ap cdp, page 345
- ap core-dump, page 346
- ap country, page 347
- ap crash-file, page 348
- ap dot11 24ghz preamble, page 349
- ap dot11 24ghz dot11g, page 349
- ap dot11 5ghz channelswitch mode, page 350
- ap dot11 5ghz power-constraint, page 351
- ap dot11 beaconperiod, page 352
- ap dot11 beamforming, page 353
- ap dot11 cac media-stream, page 354
- ap dot11 cac multimedia, page 356
- ap dot11 cac video, page 357
- ap dot11 cac voice, page 358
- ap dot11 cleanair, page 361
- ap dot11 cleanair alarm air-quality, page 362
- ap dot11 cleanair alarm device, page 363
- ap dot11 cleanair device, page 364
- ap dot11 dot11n, page 365

- ap dot11 dtpc, page 368
- ap dot11 edca-parameters, page 369
- ap dot11 rrm group-mode, page 370
- ap dot11 rrm channel cleanair-event, page 371
- ap dot11 l2roam rf-params, page 372
- ap dot11 media-stream, page 373
- ap dot11 rrm ccx location-measurement, page 374
- ap dot11 rrm channel dca, page 375
- ap dot11 rrm group-member, page 377
- ap dot11 rrm logging, page 378
- ap dot11 rrm monitor, page 379
- ap dot11 rrm ndp-type, page 380
- ap dot11 5ghz dot11ac frame-burst, page 381
- ap dot1x max-sessions, page 382
- ap dot1x username, page 382
- ap ethernet duplex, page 383
- ap group, page 384
- ap image, page 385
- ap ipv6 tcp adjust-mss, page 386
- ap led, page 387
- ap link-encryption, page 387
- ap link-latency, page 388
- ap mgmtuser username, page 388
- ap name ap-groupname, page 390
- ap name antenna band mode, page 391
- ap name bhrate, page 391
- ap name bridgegroupname, page 392
- ap name bridging, page 393
- ap name cdp interface, page 393
- ap name console-redirect, page 394
- ap name capwap retransmit, page 395
- ap name command, page 396
- ap name core-dump, page 396

- ap name country, page 397
- ap name crash-file, page 398
- ap name dot11 24ghz rrm coverage, page 399
- ap name dot11 49ghz rrm profile, page 400
- ap name dot11 5ghz rrm channel, page 402
- ap name dot11 antenna, page 402
- ap name dot11 antenna extantgain, page 404
- ap name dot11 cleanair, page 404
- ap name dot11 dot11n antenna, page 405
- ap name dot11 dual-band cleanair, page 406
- ap name dot11 dual-band shutdown, page 407
- ap name dot11 rrm ccx, page 407
- ap name dot11 rrm profile, page 408
- ap name dot11 txpower, page 410
- ap name dot1x-user, page 411
- ap name ethernet, page 412
- ap name ethernet duplex, page 413
- ap name key-zeroize , page 414
- ap name image, page 414
- ap name ipv6 tcp adjust-mss, page 415
- ap name jumbo mtu, page 416
- ap name lan, page 416
- ap name led, page 417
- ap name link-encryption, page 418
- ap name link-latency, page 418
- ap name location, page 419
- ap name mgmtuser, page 420
- ap name mode, page 421
- ap name monitor-mode, page 422
- ap name monitor-mode dot11b, page 423
- ap name name, page 424
- ap name no dot11 shutdown, page 424
- ap name power, page 425

- ap name shutdown, page 426
- ap name slot shutdown, page 426
- ap name sniff, page 427
- ap name ssh, page 428
- ap name telnet, page 429
- ap name power injector, page 429
- ap name power pre-standard, page 430
- ap name reset-button, page 431
- ap name reset, page 431
- ap name slot, page 432
- ap name static-ip, page 433
- ap name stats-timer, page 434
- ap name syslog host, page 435
- ap name syslog level, page 436
- ap name tcp-adjust-mss, page 437
- ap name tftp-downgrade, page 438
- ap power injector, page 438
- ap power pre-standard, page 439
- ap reporting-period, page 440
- ap reset-button, page 440
- service-policy type control subscriber, page 441
- ap static-ip, page 442
- ap syslog, page 442
- ap name no controller , page 444
- ap tcp-adjust-mss size, page 445
- ap tftp-downgrade, page 445
- config wireless wps rogue client mse, page 446
- clear ap name tsm dot11 all, page 447
- clear ap config, page 448
- clear ap eventlog-all, page 448
- clear ap join statistics, page 449
- clear ap mac-address, page 449
- clear ap name wlan statistics, page 450

- debug ap mac-address, page 451
- show ap cac voice, page 451
- show ap capwap, page 452
- show ap cdp, page 454
- show ap config dot11, page 454
- show ap config dot11 dual-band summary, page 455
- show ap config fnf, page 456
- show ap config, page 456
- show ap crash-file, page 457
- show ap data-plane, page 457
- show ap dot11 l2roam, page 458
- show ap dot11 cleanair air-quality, page 459
- show ap dot11 cleanair config, page 460
- show ap dot11 cleanair summary, page 461
- show ap dot11, page 461
- show ap env summary, page 466
- show ap ethernet statistics, page 467
- show ap gps-location summary, page 467
- show ap groups, page 468
- show ap groups extended, page 468
- show ap image, page 469
- show ap is-supported, page 469
- show ap join stats summary, page 470
- show ap link-encryption, page 471
- show ap mac-address, page 471
- show ap monitor-mode summary, page 473
- show ap name auto-rf, page 473
- show ap name bhmode, page 475
- show ap name bhrate, page 476
- show ap name cac voice, page 476
- show ap name config fnf, page 477
- show ap name dot11 call-control, page 478
- show ap name cable-modem, page 479

- show ap name capwap retransmit, page 479
- show ap name ccx rm, page 480
- show ap name cdp, page 481
- show ap name channel, page 481
- show ap name config, page 482
- show ap name config dot11, page 484
- show ap name config slot, page 487
- show ap name core-dump, page 490
- show ap name data-plane, page 491
- show ap name dot11, page 491
- show ap name dot11 cleanair, page 494
- show ap name env, page 495
- show ap name ethernet statistics, page 495
- show ap name eventlog, page 496
- show ap gps-location summary, page 497
- show ap name image, page 497
- show ap name inventory, page 498
- show ap name lan port, page 499
- show ap name link-encryption, page 499
- show ap name service-policy, page 500
- show ap name tcp-adjust-mss, page 501
- show ap name wlan, page 501
- show ap name wlandot11 service policy, page 502
- show ap slots, page 503
- show ap summary, page 504
- show ap tcp-adjust-mss, page 504
- show ap universal summary, page 505
- show ap uptime, page 505
- show wireless ap summary, page 506
- show wireless client ap, page 507
- test ap name, page 508
- test capwap ap name, page 508
- trapflags ap, page 509

ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the device, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the device, use the **no** form of this command.

ap auth-list ap-policy {**authorize-ap**| **lsc**| **mic**| **ssc**}

no ap auth-list ap-policy {**authorize-ap**| **lsc**| **mic**| **ssc**}

Syntax Description

authorize-ap	Enables the authorization policy.
lsc	Enables access points with locally significant certificates to connect.
mic	Enables access points with manufacture-installed certificates to connect.
ssc	Enables access points with self signed certificates to connect.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the access point authorization policy:

```
Device(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Device(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Device(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Device(config)# ap auth-list ap-policy ssc
```

ap bridging

To enable Ethernet to 802.11 bridging on a Cisco lightweight access point, use the **ap bridging** command. To disable Ethernet to 802.11 bridging on a Cisco lightweight access point, use the **no** form of this command.

ap bridging

no ap bridging

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable Ethernet-to-Ethernet bridging on a lightweight access point:

```
Device(config)# ap bridging
```

This example shows how to disable Ethernet-to-Ethernet bridging on a lightweight access point:

```
Device(config)# no ap bridging
```

ap capwap multicast

To configure the multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled and to configure the outer Quality of Service (QoS) level of those multicast packets sent to the access points, use the **ap capwap multicast** command.

ap capwap multicast {*multicast-ip-address*| **service-policy output** *pollicymap-name*}

Syntax Description

multicast-ip-address	Multicast IP address.
service-policy	Specifies the tunnel QoS policy for multicast access points.
output	Assigns a policy map name to the output.
policymap-name	Service policy map name.

Command Default

None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a multicast address used by all access points to receive multicast traffic when multicast forwarding is enabled:

```
Device(config)# ap capwap multicast 239.2.2.2
```

This example shows how to configure a tunnel multicast QoS service policy for multicast access points:

```
Device(config)# ap capwap multicast service-policy output tunnmulpolicy
```

ap capwap retransmit

To configure Control and Provisioning of Wireless Access Points (CAPWAP) control packet retransmit count and control packet retransmit interval, use the **ap capwap retransmit** command.

ap capwap retransmit {**count** *retransmit-count*| **interval** *retransmit-interval*}

Syntax Description

count *retransmit-count*	Specifies the access point CAPWAP control packet retransmit count. **Note** The count is from 3 to 8 seconds.
interval *retransmit-interval*	Specifies the access point CAPWAP control packet retransmit interval. **Note** The interval is from 2 to 5 seconds.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the CAPWAP control packet retransmit count for an access point:

```
Device# ap capwap retransmit count 3
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Device# ap capwap retransmit interval 5
```

ap capwap timers

To configure advanced timer settings, use the **ap capwap timers** command.

ap capwap timers {**discovery-timeout** *seconds*| **fast-heartbeat-timeout local** *seconds*| **heartbeat-timeout** *seconds*| **primary-discovery-timeout** *seconds*| **primed-join-timeout** *seconds*}

Syntax Description

discovery-timeout	Specifies the Cisco lightweight access point discovery timeout. **Note** The Cisco lightweight access point discovery timeout is how long a Cisco device waits for an unresponsive access point to answer before considering that the access point failed to respond.
seconds	Cisco lightweight access point discovery timeout from 1 to 10 seconds. **Note** The default is 10 seconds.
fast-heartbeat-timeout local	Enables the fast heartbeat timer that reduces the amount of time it takes to detect a device failure for local or all access points.
seconds	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a device failure. **Note** The fast heartbeat time-out interval is disabled by default.
heartbeat-timeout	Specifies the Cisco lightweight access point heartbeat timeout. **Note** The Cisco lightweight access point heartbeat timeout controls how often the Cisco lightweight access point sends a heartbeat keep-alive signal to the Cisco device. This value should be at least three times larger than the fast heartbeat timer.
seconds	Cisco lightweight access point heartbeat timeout value from 1 to 30 seconds. **Note** The default is 30 seconds.
primary-discovery-timeout	Specifies the access point primary discovery request timer. The timer determines the amount of time taken by an access point to discovery the configured primary, secondary, or tertiary device.
seconds	Access point primary discovery request timer from 30 to 3600 seconds. **Note** The default is 120 seconds.

primed-join-timeout	Specifies the authentication timeout. Determines the time taken by an access point to determine that the primary device has become unresponsive. The access point makes no further attempts to join the device until the connection to the device is restored.
seconds	Authentication response timeout from 120 to 43200 seconds. **Note** The default is 120 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure an access point discovery timeout with the timeout value of 7:

```
Device(config)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Device(config)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Device(config)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Device(config)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Device(config)# ap capwap timers primed-join-timeout 360
```

ap cdp

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **ap cdp** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

no ap cdp [**interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}]

Syntax Description

interface	(Optional) Specifies CDP in a specific interface.

ethernet	Specifies CDP for an Ethernet interface.
ethernet-id	Ethernet interface number from 0 to 3.
radio	Specifies CDP for a radio interface.
radio-id	Radio number from 0 to 3.

Command Default

Disabled on all access points.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no ap cdp** command disables CDP on all access points that are joined to the device and all access points that join in the future. CDP remains disabled on both current and future access points even after the device or access point reboots. To enable CDP, enter the **ap cdp** 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 device, you can disable and then reenable CDP on individual access points using the **ap name** *Cisco-AP* **cdp** command. After you disable CDP on all access points joined to the device, you can enable and then disable CDP on individual access points.

This example shows how to enable CDP on all access points:

```
Device(config)# ap cdp
```

This example shows how to enable CDP for Ethernet interface number 0 on all access points:

```
Device(config)# ap cdp ethernet 0
```

ap core-dump

To enable a Cisco lightweight access point's memory core dump settings, use the **ap core-dump** command. To disable a Cisco lightweight access point's memory core dump settings, use the **no** form of this command.

ap core-dump *tftp-ip-addr filename* {**compress**| **uncompress**}

no ap core-dump

Syntax Description

tftp-ip-addr	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.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The access point must be able to reach the TFTP server.

This example shows how to configure and compress the core dump file:

```
Device(config)# ap core-dump 192.0.2.51 log compress
```

ap country

To configure one or more country codes for a device, use the **ap country** command.

ap country *country-code*

Syntax Description

country-code	Two-letter or three-letter country code or several country codes separated by a comma.

Command Default

US (country code of the United States of America).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco device 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 to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains.

This example shows how to configure country codes on the device to IN (India) and FR (France):

```
Device(config)# ap country IN,FR
```

ap crash-file

To delete crash and radio core dump files, use the **ap crash-file** command.

ap crash-file {**clear-all**| **delete** *filename*}

Syntax Description

clear-all	Deletes all the crash and radio core dump files.
delete	Deletes a single crash and radio core dump file.
filename	Name of the file to delete.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to delete all crash files:

```
Device# ap crash-file clear-all
```

This example shows how to delete crash file 1:

```
Device# ap crash-file delete crash-file-1
```

ap dot11 24ghz preamble

To enable only a short preamble as defined in subclause 17.2.2.2 , use the **ap dot11 24ghz preamble** command. To enable long preambles (for backward compatibility with pre-802.11b devices, if these devices are still present in your network) or short preambles (recommended unless legacy pre-802.11b devices are present in the network), use the **no** form of this command.

ap dot11 24ghz preamble short

no ap dot11 24ghz preamble short

Syntax Description

short	Specifies the short 802.11b preamble.

Command Default

short preambles

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Note You must reboot the Cisco device (reset system) with the **Save** command before you can use the **ap dot11 24ghz preamble** command.

This parameter may need to be set to long to optimize this Cisco device for some legacy clients, including SpectraLink NetLink telephones.

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

This example shows how to enable both long and short preamblest:

```
Device(config)# no ap dot11 24ghz preamble short
```

ap dot11 24ghz dot11g

To enable the Cisco wireless LAN solution 802.11g network, use the **ap dot11 24ghz dot11g** command. To disable the Cisco wireless LAN solution 802.11g network, use the **no** form of this command.

ap dot11 24ghz dot11g

no ap dot11 24ghz dot11g

Syntax Description

This command has no keywords and arguments.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you enter the **ap dot11 24ghz dot11g** command, disable the 802.11 Cisco radio with the **ap dot11 24ghz shutdown** command.

After you configure the support for the 802.11g network, use the **no ap dot11 24ghz shutdown** command to enable the 802.11 2.4 Ghz radio.

This example shows how to enable the 802.11g network:

```
Device(config)# ap dot11 24ghz dot11g
```

ap dot11 5ghz channelswitch mode

To configure a 802.11h channel switch announcement, use the **ap dot11 5ghz channelswitch mode** command. To disable a 802.11h channel switch announcement, use the **no** form of this command.

ap dot11 5ghz channelswitch mode *value*

no ap dot11 5ghz channelswitch mode

Syntax Description

value 802.11h channel announcement value.

Note You can specify anyone of the following two values:

- 0—Indicates that the channel switch announcement is disabled.
- 1—Indicates that the channel switch announcement is enabled.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the 802.11h switch announcement:

```
Device(config)# ap dot11 5ghz channelswitch mode 1
```

ap dot11 5ghz power-constraint

To configure the 802.11h power constraint value, use the **ap dot11 5ghz power-constraint** command. To remove the 802.11h power constraint value, use the **no** form of this command.

ap dot11 5ghz power-constraint *value*

no ap dot11 5ghz power-constraint

Syntax Description

value	802.11h power constraint value. **Note** The range is from 0 to 30 dBm.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the 802.11h power constraint to 5 dBm:

```
Device(config)# ap dot11 5ghz power-constraint 5
```

ap dot11 beaconperiod

To change the beacon period globally for 2.4 GHz or 5 GHz bands, use the **ap dot11 beaconperiod** command.

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

ap dot11 {**24ghz**| **5ghz**} **beaconperiod** *time*

Syntax Description

24ghz	Specifies the settings for 2.4 GHz band.
5ghz	Specifies the settings for 5 GHz band.
beaconperiod	Specifies the beacon for a network globally.
time	Beacon interval in time units (TU). One TU is 1024 microseconds. The range is from 20 to 1000.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In Cisco wireless LAN 802.11 networks, all Cisco lightweight access point wireless LANs broadcast a beacon at regular intervals. This beacon notifies clients that the wireless 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 **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After changing the beacon period, enable the 802.11 network by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to configure the 5 GHZ band for a beacon period of 120 time units:

```
Device(config)# ap dot11 5ghz beaconperiod 120
```

ap dot11 beamforming

To enable beamforming on the network or on individual radios, use the **ap dot11 beamforming** command.

ap dot11 {**24ghz**| **5ghz**} **beamforming**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
beamforming	Specifies beamforming on the network.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 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 Direct Sequence Spread Spectrum data rates (1 and 2 Mbps) and Complementary-Code Key (CCK) data rates (5.5 and 11 Mbps).

- Beamforming is supported only on access points that support 802.11n (AP1260, AP3500, and AP3600).
- 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.

This example shows how to enable beamforming on the 5 GHz band:

```
Device(config)# ap dot11 5ghz beamforming
```

ap dot11 cac media-stream

To configure media stream Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac media-stream** command.

ap dot11 {**24ghz**| **5ghz**} **cac media-stream multicast-direct** {**max-retry-percent** *retryPercent*| **min-client-rate**{**eighteen**| **eleven**| **fiftyFour**| **fivePointFive**| **fortyEight**| **nine**| **oneFifty**| **oneFortyFourPointFour**| **oneThirty**| **oneThirtyFive**| **seventyTwoPointTwo**| **six**| **sixtyFive**| **thirtySix**| **threeHundred**| **twelve**| **twentyFour**| **two**| **twoSeventy**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies CAC parameters for multicast-direct media streams.
max-retry-percent	Specifies the percentage of maximum retries that are allowed for multicast-direct media streams.
retryPercent	Percentage of maximum retries that are allowed for multicast-direct media streams. **Note** The range is from 0 to 100.
min-client-rate	Specifies the minimum transmission data rate to the client for multicast-direct media streams (rate at which the client must transmit in order to receive multicast-direct unicast streams). If the transmission 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.

min-client-rate	You can choose the following rates: • **eighteen** • **eleven** • **fiftyFour** • **fivePointFive** • **fortyEight** • **nine** • **one** • **oneFifty** • **oneFortyFourPointFour** • **oneThirty** • **oneThirtyFive** • **seventyTwoPointTwo** • **six** • **sixtyFive** • **thirtySix** • **threeHundred** • **twelve** • **twentyFour** • **two** • **twoSeventy**

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.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

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

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

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

```
Device(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

ap dot11 cac multimedia

To configure multimedia Call Admission Control (CAC) voice and video quality parameters for 2.4 GHz and 5 GHz bands, use the **ap dot11 cac multimedia** command.

ap dot11 {**24ghz| 5ghz**} **cac multimedia max-bandwidth** *bandwidth*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
max-bandwidth	Specifies the percentage of maximum bandwidth allocated to Wi-Fi Multimedia (WMM) clients for voice and video applications on the 2.4 GHz or 5 GHz band.
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 multimedia flows this radio band. The range is from 5 to 85%.

Command Default

The default value is 75%.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

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

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

This example shows how to configure the percentage of the maximum bandwidth allocated to WMM clients for voice and video applications on the 5 GHz band:

```
Device(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

ap dot11 cac video

To configure Call Admission Control (CAC) parameters for the video category, use the **ap dot11 cac video** command. To disable the CAC parameters for video category, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

no ap dot11 {**24ghz**| **5ghz**} **cac video** {**acm**| **max-bandwidth** *value*| **roam-bandwidth** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based video CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based video CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz	5ghz**} **cac video acm** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for video applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.

roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming video clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CAC commands require that the WLAN you are planning to modify is configured for the Wi-Fi Multimedia (WMM) protocol.

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

- Disable all WLANs with WMM enabled by entering the **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** command.

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

```
Device(config)# ap dot11 24ghz cac video acm
```

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

```
Device(config)# ap dot11 24ghz cac video max-bandwidth 50
```

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

```
Device(config)# ap dot11 24ghz cac video roam-bandwidth 10
```

ap dot11 cac voice

To configure Call Admission Control (CAC) parameters for the voice category, use the **ap dot11 cac voice** command.

ap dot11 {**24ghz**| **5ghz**} **cac voice**{**acm**| **load-based**| **max-bandwidth** *value*| **roam-bandwidth** *value*| **sip** [**bandwidth** *bw*] **sample-interval** *value*| **stream-size** *x* **max-streams** *y*| **tspec-inactivity-timeout**{**enable**| **ignore**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
acm	Enables bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band. **Note** To disable bandwidth-based voice CAC for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice acm** command.
load-based	Enable load-based CAC on voice access category. **Note** To disable load-based CAC on voice access category for the 2.4 GHz or 5 GHz band, use the **no ap dot11** {**24ghz | 5ghz**} **cac voice load-based** command.
max-bandwidth	Sets the percentage of the maximum bandwidth allocated to clients for voice applications on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 5 to 85%.
roam-bandwidth	Sets the percentage of the CAC maximum allocated bandwidth reserved for roaming voice clients on the 2.4 GHz or 5 GHz band.
value	Bandwidth percentage value from 0 to 85%.
sip	Specifies the CAC codec name and sample interval as parameters and calculates the required bandwidth per call for the 802.11 networks.
bandwidth	(Optional) Specifies bandwidth for a SIP-based call.
bw	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: • 64kbps—Specifies CAC parameters for the SIP G711 codec. • 8kbps—Specifies CAC parameters for the SIP G729 codec. **Note** The default value is 64 Kbps.
sample-interval	Specifies the packetization interval for SIP codec.

value	Packetization interval in msecs. The sample interval for SIP codec value is 20 seconds.
stream-size	Specifies the number of aggregated voice Wi-Fi Multimedia (WMM) traffic specification (TSPEC) streams at a specified data rate for the 2.4 GHz or 5 GHz band.
x	Stream size. The range of the stream size is from 84000 to 92100.
max-streams	Specifies the maximum number of streams per TSPEC.
y	Number (1 to 5) of voice streams. **Note** The default number of streams is 2 and the mean data rate of a stream is 84 kbps.
tspec-inactivity-timeout	Specifies TSPEC inactivity timeout processing mode. **Note** Use this keyword to process or ignore the Wi-Fi Multimedia (WMM) traffic specifications (TSPEC) inactivity timeout received from an access point. When the inactivity timeout is ignored, a client TSPEC is not deleted even if the access point reports an inactivity timeout for that client.
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages. **Note** The default is **ignore** (disabled).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 **wlan** *wlan_name* **shutdown** command.
- Disable the radio network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.
- Save the new configuration.
- Enable voice or video CAC for the network you want to configure by entering the **ap dot11** {**24ghz | 5ghz**} **cac voice acm** or **ap dot11** {**24ghz | 5ghz**} **cac video acm** commands.

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

```
Device(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Device(config)# ap dot11 24ghz cac voice load-based
```

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

```
Device(config)# ap dot11 24ghz cac voice max-bandwidth 50
```

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

```
Device(config)# ap dot11 24ghz cac voice roam-bandwidth 10
```

This example shows how to configure the bandwidth and voice packetization interval for the G729 SIP codec on a 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cac voice sip bandwidth 8 sample-interval 40
```

This example shows how to configure the number of aggregated voice traffic specifications stream with a stream size of 85000 and with a maximum of 5 streams:

```
Device(config)# ap dot11 24ghz cac voice stream-size 85000 max-streams 5
```

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

```
Device(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

ap dot11 cleanair

To configure CleanAir on 802.11 networks, use the **ap dot11 cleanair** command. To disable CleanAir on 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cleanair**

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
cleanair	Specifies CleanAir on the 2.4 GHz or 5 GHz band.

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the CleanAir settings on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz cleanair
```

ap dot11 cleanair alarm air-quality

To configure CleanAir air-quality alarms for Cisco lightweight access points, use the **ap dot11 cleanair alarm air-quality** command.

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm air-quality** [**threshold** *value*]

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
threshold	Specifies the air-quality alarm threshold.
value	Air quality alarm threshold (1 is bad air quality, and 100 is good air quality).

Command Default Disabled

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the CleanAir 2.4 GHz air-quality threshold to 90:

```
Device(config)# ap dot11 24ghz cleanair air-quality threshold 90
```

ap dot11 cleanair alarm device

To configure the CleanAir interference devices alarms on the 2.4 GHz or 5 GHz bands, use the **ap dot11 cleanair alarm device** command. To disable the CleanAir interference devices alarms on the 802.11 networks, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **cleanair alarm device**{**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**}

no ap dot11 {**24ghz**| **5ghz**} **cleanair**

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
all	Specifies all the device types at once.
bt-discovery	Specifies the Bluetooth device in discovery mode.
bt-link	Specifies the Bluetooth active link.
canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.
fh	Specifies the frequency hopping devices.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
mw-oven	Specifies the microwave oven devices.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.

wimax-mobile	Specifies a WiMax mobile device.
xbox	Specifies the Xbox device.
zigbee	Specifies the ZigBee device.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable alarms for ZigBee interference detection:

```
Device(config)# no ap dot11 24ghz cleanair alarm device zigbee
```

This example shows how to enable alarms for detection of Bluetooth links:

```
Device(config)# ap dot11 24ghz cleanair alarm device bt-link
```

ap dot11 cleanair device

To configure CleanAir interference device types, use the **ap dot11 cleanair device** command.

ap dot11 24ghz cleanair device [**all**| **bt-discovery**| **bt-link**| **canopy**| **cont-tx**| **dect-like**| **fh**| **inv**| **jammer**| **mw-oven**| **nonstd**| **superag**| **tdd-tx**| **video**| **wimax-fixed**| **wimax-mobile**| **xbox**| **zigbee**]

Syntax Description

all	Specifies all device types.
device	Specifies the CleanAir interference device type.
bt-discovery	Specifies the Bluetooth device in discovery mode.
bt-link	Specifies the Bluetooth active link.
canopy	Specifies the Canopy devices.
cont-tx	Specifies the continuous transmitter.
dect-like	Specifies a Digital Enhanced Cordless Communication (DECT)-like phone.

fh	Specifies the 802.11 frequency hopping devices.
inv	Specifies the devices using spectrally inverted Wi-Fi signals.
jammer	Specifies the jammer.
mw-oven	Specifies the microwave oven devices.
nonstd	Specifies the devices using nonstandard Wi-Fi channels.
superag	Specifies 802.11 SuperAG devices.
tdd-tx	Specifies the TDD transmitter.
video	Specifies video cameras.
wimax-fixed	Specifies a WiMax fixed device.
wimax-mobile	Specifies a WiMax mobile device.
xbox	Specifies the Xbox device.
zigbee	Specifies the ZigBee device.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the device to monitor ZigBee interferences:

```
Device(config)# ap dot11 24ghz cleanair device zigbee
```

ap dot11 dot11n

To configure settings for an 802.11n network, use the **ap dot11 dot11n** command.

ap dot11 {**24ghz**| **5ghz**} **dot11n** {**a-mpdu tx priority** {*priority_value* **all** }| **scheduler timeout rt** *scheduler_value*}| **a-msdu tx priority** {*priority_value*| **all**}| **guard-interval** {**any**| **long**}| **mcs tx** *rate*| **rifs rx**}

Syntax Description

24ghz	Specifies the 2.4-GHz band.
5ghz	Specifies the 5-GHz band.
dot11n	Enables 802.11n support.
a-mpdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Protocol Data Unit (A-MPDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
a-msdu tx priority	Specifies the traffic that is associated with the priority level that uses Aggregated MAC Service Data Unit (A-MSDU) transmission.
priority_value	Aggregated MAC protocol data unit priority level from 0 to 7.
all	Specifies all of the priority levels at once.
scheduler timeout rt	Configures the 802.11n A-MPDU transmit aggregation scheduler timeout value in milliseconds.
scheduler_value	The 802.11n A-MPDU transmit aggregation scheduler timeout value from 1 to 10000 milliseconds.
guard-interval	Specifies the guard interval.
any	Enables either a short or a long guard interval.
long	Enables only a long guard interval.
mcs tx *rate*	Specifies the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client.
rate	Specifies the modulation and coding scheme data rates. **Note** The range is from 0 to 23.
rifs rx	Specifies the Reduced Interframe Space (RIFS) between data frames.

Command Default

By default, priority 0 is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The scheduler, timeout, and rt keywords were added.

Usage Guidelines

Aggregation is the process of grouping packet data frames together rather than transmitting them separately. The two aggregation methods available are:

- A-MPDU—This aggregation is performed in the software.
- A-MSDU—This aggregation is performed in the hardware

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

- 0—Best effort
- 1—Background
- 2—Spare
- 3—Excellent effort
- 4—Controlled load
- 5—Video, less than 100-ms latency and jitter
- 6—Voice, less than 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.

This example shows how to enable 802.11n support on a 2.4-GHz band:

```
Device(config)# ap dot11 24ghz dot11n
```

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

```
Device(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Device(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Device(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Device(config)# ap dot11 24ghz dot11n rifs rx
```

ap dot11 dtpc

To configure Dynamic Transmit Power Control (DTPC) settings, Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature, and the fragmentation threshold on an 802.11 network, use the **ap dot11 dtpc** command.

ap dot11 {**24ghz**| **5ghz**} {**dtpc**| **exp-bwreq**| **fragmentation** *threshold*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
dtpc	Specifies Dynamic Transport Power Control (DTPC) settings. **Note** This option is enabled by default.
exp-bwreq	Specifies Cisco Client eXtension (CCX) version 5 expedited bandwidth request feature. **Note** The expedited bandwidth request feature is disabled by default.
fragmentation *threshold*	Specifies the fragmentation threshold. **Note** This option can only used be when the network is disabled using the **ap dot11** {**24ghz** | **5ghz**} **shutdown** command.
threshold	Threshold. The range is from 256 to 2346 bytes (inclusive).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the CCX version 5 expedited bandwidth request feature is enabled, the device configures all joining access points for this feature.

This example shows how to enable DTPC for the 5 GHz band:

```
Device(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Device(config)# ap dot11 5ghz exp-bwrep
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Device(config)# ap dot11 5ghz fragmentation 1500
```

ap dot11 edca-parameters

To enable a specific enhanced distributed channel access (EDCA) profile on the 2.4 GHz or 5 GHz bands, use the **ap dot11 edca-parameters** command. To disable an EDCA profile on the 2.4 GHz or 5 GHz bands, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

no ap dot11 {**24ghz**| **5ghz**} **edca-parameters** {**custom-voice**| **optimized-video-voice**| **optimized-voice**| **svp-voice**| **wmm-default**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
edca-parameters	Specifies a specific enhanced distributed channel access (EDCA) profile on the 802.11 networks.
custom-voice	Enables custom voice EDCA parameters.
optimized-video-voice	Enables EDCA voice- and video-optimized profile parameters. Choose this option when both voice and video services are deployed on your network.
optimized-voice	Enables EDCA voice-optimized profile parameters. Choose this option when voice services other than SpectraLink are 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.
wmm-default	Enables the Wi-Fi Multimedia (WMM) default parameters. Choose this option when voice or video services are not deployed on your network.

Command Default

wmm-default

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
10.3	The **custom-voice** keyword was removed for Cisco 5700 Series WLC.

This example shows how to enable SpectraLink voice priority parameters:

```
Device(config)# ap dot11 24ghz edca-parameters svp-voice
```

ap dot11 rrm group-mode

To set the 802.11 automatic RF group selection mode on, use the **ap dot11 rrm group-mode** command. To set the 802.11 automatic RF group selection mode off, use the **no** form of this command.

ap dot11 {**5ghz**| **24ghz**} **rrm group-mode** {**auto**| **leader**| **off**| **restart**}

no ap dot11 {**5ghz**| **24ghz**} **rrm group-mode**

Syntax Description

5ghz	Specifies the 2.4 GHz band.
24ghz	Specifies the 5 GHz band.
auto	Sets the 802.11 RF group selection to automatic update mode.
leader	Sets the 802.11 RF group selection to static mode, and sets this device as the group leader.
off	Sets the 802.11 RF group selection to off.

restart	Restarts the 802.11 RF group selection.

Command Default

auto

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to turn the auto RF group selection mode on the 5 GHz band:

```
Device(config)# ap dot11 5ghz rrm group-mode auto
```

ap dot11 rrm channel cleanair-event

To configure CleanAir event-driven Radio Resource Management (RRM) parameters for all 802.11 Cisco lightweight access points, use the **ap dot11 rrm channel cleanair-event** command. When this parameter is configured, CleanAir access points can change their channel when a source of interference degrades the operations, even if the RRM interval has not expired yet.

ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event sensitivity** *value*}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
sensitivity	Sets the sensitivity for CleanAir event-driven RRM.
value	Sensitivity value. You can specify any one of the following three optional sensitivity values: • **low—**Specifies low sensitivity. • **medium—**Specifies medium sensitivity. • **high—**Specifies high sensitivity.

Command Default

None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the high sensitivity for CleanAir event-driven RRM:

```
Device(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

ap dot11 l2roam rf-params

To configure the 2.4 GHz or 5 GHz Layer 2 client roaming parameters, use the **ap dot11 l2roam rf-params** command.

ap dot11 {**24ghz**| **5ghz**} **l2roam rf-params custom** *min-rssi roam-hyst scan-thresh trans-time*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
custom	Specifies custom Layer 2 client roaming RF parameters.
min-rssi	Minimum received signal strength indicator (RSSI) that is required for the client to associate to the access point. If the client's average received signal power dips below this threshold, reliable communication is usually impossible. Clients must already have found and roamed to another access point with a stronger signal before the minimum RSSI value is reached. The valid range is –80 to –90 dBm, and the default value is –85 dBm.
roam-hyst	How much greater the signal strength of a neighboring access point must be in order for the client to roam to it. This parameter is intended to reduce the amount of roaming between access points if the client is physically located on or near the border between the two access points. The valid range is 2 to 4 dB, and the default value is 2 dB.
scan-thresh	Minimum RSSI that is allowed before the client should roam to a better access point. When the RSSI drops below the specified value, the client must be able to roam to a better access point within the specified transition time. This parameter also provides a power-save method to minimize the time that the client spends in active or passive scanning. For example, the client can scan slowly when the RSSI is above the threshold and scan more rapidly when the RSSI is below the threshold. The valid range is –70 to –77 dBm, and the default value is –72 dBm.

trans-time	Maximum time allowed for the client to detect a suitable neighboring access point to roam to and to complete the roam, whenever the RSSI from the client's associated access point is below the scan threshold. The valid range is 1 to 10 seconds, and the default value is 5 seconds.

Command Default

min-rssi	-85
roam-hyst	2
scan-thresh	-72
trans-time	5

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure custom Layer 2 client roaming parameters on an 802.11a network:

```
Device(config)# ap dot11 5ghz l2roam rf-params custom -80 2 -70 7
```

ap dot11 media-stream

To configure media stream multicast-direct and video-direct settings on an 802.11 network, use the **ap dot11 media-stream** command.

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
multicast-direct	Specifies the multicast-direct for the 2.4 GHz or a 5 GHz band.
admission-besteffort	Admits the media stream to the best-effort queue.
client-maximum *value*	Specifies the maximum number of streams allowed on a client.

radio-maximum *value*	Specifies the maximum number of streams allowed on a 2.4 GHz or a 5 GHz band.
video-redirect	Specifies the media stream video-redirect for the 2.4 GHz or a 5 GHz band.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure the media stream multicast-direct or video-redirect on a 802.11 network, ensure that the network is nonoperational.

This example shows how to enable media stream multicast-direct settings on the 5 GHz band:

```
Device(config)# ap dot11 5ghz media-stream multicast-direct
```

This example shows how to admit the media stream to the best-effort queue if there is not enough bandwidth to prioritize the flow:

```
Device(config)# ap dot11 5ghz media-stream multicast-direct admission-besteffort
```

This example shows how to set the maximum number of streams allowed on a client:

```
Device(config)# ap dot11 5ghz media-stream multicast-direct client-maximum 10
```

This example shows how to enable media stream traffic redirection on the 5 GHz band:

```
Device(config)# ap dot11 5ghz media-stream video-redirect
```

ap dot11 rrm ccx location-measurement

To configure cisco client Extensions (CCX) client location measurements for 2.4 GHz and 5 GHz bands, use the **ap dot11 rrm ccx location-measurement** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ccx location-measurement** {**disable**| *interval*}

Syntax Description

24ghz	Specifies the 2.4-GHz band.

5ghz	Specifies the 5-GHz band.
disable	Disables support for CCX client location measurements.
interval	Interval from 10 to 32400.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable support for 2.4 GHz CCX client location measurements:

```
Device(config)# no ap dot11 24ghz rrm ccx location-measurement
```

ap dot11 rrm channel dca

To configure Dynamic Channel Assignment (DCA) algorithm parameters on 802.11 networks, use the **ap dot11 rrm channel dca** command.

ap dot11 {**24ghz**| **5ghz**} **rrm channel dca**{*channel_number*| **anchor-time** *value*| **global**{**auto**| **once**}| **interval** *value*| **min-metric** *value*| **sensitivity**{**high**| **low**| **medium**}}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel_number	Channel number to be added to the DCA list. **Note** The range is from 1 to 14.
anchor-time	Specifies the anchor time for DCA.
value	Hour of time between 0 and 23. These values represent the hour from 12:00 a.m. to 11:00 p.m.
global	Specifies the global DCA mode for the access points in the 802.11 networks.
auto	Enables auto-RF.

once	Enables one-time auto-RF.
interval	Specifies how often the DCA is allowed to run.
value	Interval between the times when DCA is allowed to run. Valid values are 0, 1, 2, 3, 4, 6, 8, 12, or 24 hours. 0 is 10 minutes (600 seconds). Default value is 0 (10 minutes).
min-metric	Specifies the DCA minimum RSSI energy metric.
value	Minimum RSSI energy metric value from –100 to –60.
sensitivity	Specifies how sensitive the DCA algorithm is to environmental changes (for example, signal, load, noise, and interference) when determining whether or not to change channels.
high	Specifies that the DCA algorithm is not particularly sensitive to environmental changes. See the “Usage Guidelines” section for more information.
low	Specifies that the DCA algorithm is moderately sensitive to environmental changes. See the “Usage Guidelines” section for more information.
medium	Specifies that the DCA algorithm is highly sensitive to environmental changes. See the “Usage Guidelines” section for more information.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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. The table below explains the possible error codes for failed calls.

Table 22: DCA Sensitivity Threshold

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
High	5 dB	5 dB

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
Medium	15 dB	20 dB
Low	30 dB	35 dB

This example shows how to configure the device to start running DCA at 5 pm for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca anchor-time 17
```

This example shows how to set the DCA algorithm to run every 10 minutes for the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca interval 0
```

This example shows how to configure the value of DCA algorithm's sensitivity to low on the 2.4 GHz band:

```
Device(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

ap dot11 rrm group-member

To configure members in an 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove members from 802.11 RF group, use the **no** form of this command.

ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
controller-name	Name of the device to be added.
controller-ip	IP address of the device to be added.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to add a device in the 5 GHz band RF group:

```
Device(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

ap dot11 rrm logging

To configure report log settings on supported 802.11 networks, use the **ap dot11 rrm logging** command.

ap dot11 {**24ghz**| **5ghz**} **rrm logging** {**channel**| **coverage**| **foreign**| **load**| **noise**| **performance**| **txpower**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Turns the channel change logging mode on or off. The default mode is off (Disabled).
coverage	Turns the coverage profile logging mode on or off. The default mode is off (Disabled).
foreign	Turns the foreign interference profile logging mode on or off. The default mode is off (Disabled).
load	Turns the load profile logging mode on or off. The default mode is off (Disabled).
noise	Turns the noise profile logging mode on or off. The default mode is off (Disabled).
performance	Turns the performance profile logging mode on or off. The default mode is off (Disabled).
txpower	Turns the transit power change logging mode on or off. The default mode is off (Disabled).

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to turn the 5 GHz logging channel selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Device(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Device(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Device(config)# ap dot11 5ghz rrm logging txpower
```

ap dot11 rrm monitor

To Configure monitor settings on the 802.11 networks, use the **ap dot11 rrm monitor** command.

ap dot11 {**24ghz**| **5ghz**} **rrm monitor**{**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**} *seconds*

Syntax Description

24ghz	Specifies the 802.11b parameters.
5ghz	Specifies the 802.11a parameters.
channel-list all	Monitors the noise, interference, and rogue monitoring channel list for all channels.
channel-list country	Monitors the noise, interference, and rogue monitoring channel list for the channels used in the configured country code.
channel-list dca	Monitors the noise, interference, and rogue monitoring channel list for the channels used by automatic channel assignment.
coverage	Specifies the coverage measurement interval.
load	Specifies the load measurement interval.
noise	Specifies the noise measurement interval.
signal	Specifies the signal measurement interval.

rssi-normalization	Configure RRM Neighbor Discovery RSSI Normalization.
seconds	Measurement interval time from 60 to 3600 seconds.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to monitor the channels used in the configured country:

```
Device(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Device(config)# ap dot11 24ghz rrm monitor coverage 60
```

ap dot11 rrm ndp-type

To configure the 802.11 access point radio resource management neighbor discovery protocol type, use the **ap dot11 rrm ndp-type** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ndp-type** {**protected**| **transparent**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
protected	Specifies the Tx RRM protected (encrypted) neighbor discovery protocol.
transparent	Specifies the Tx RRM transparent (not encrypted) neighbor discovery protocol.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure the 802.11 access point RRM neighbor discovery protocol type, ensure that you have disabled the network by entering the **ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to enable the 802.11a access point RRM neighbor discovery protocol type as protected:

```
Device(config)# ap dot11 5ghz rrm ndp-type protected
```

ap dot11 5ghz dot11ac frame-burst

To configure the 802.11ac Frame Burst use the **apdot115ghzdot11acframe-burst** command. Use the **no** forms to disable the bursting of 802.11ac A-MPDUs.

ap dot115ghzdot11acframe-burst

noap dot115ghzdot11acframe-burst

ap dot115ghzdot11acframe-burstautomatic

noap dot115ghzdot11acframe-burstautomatic

Syntax Description

5ghz	Configures the 802.11a parameters.
frame-burst	Configures the bursting of 802.11ac A-MPDUs.

Command Default

No

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.6E	This command was introduced.

Example

This is the example shows how to configure the bursting of 802.11ac A-MPDUs.

```
Deviceap dot11 5ghz
  dot11ac frame-burst
```

ap dot1x max-sessions

To configure the maximum number of simultaneous 802.1X sessions allowed per access point, use the **ap dot1x max-sessions** command.

ap dot1x max-sessions *num-of-sessions*

Syntax Description

num-of-sessions	Number of maximum 802.1X sessions initiated per AP at a time. The range is from 0 to 255, where 0 indicates unlimited.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

It is required to limit the number of simultaneous 802.1X sessions initiated per access point to protect against flooding attacks caused by using 802.1X messages.

This example shows how to configure the maximum number of simultaneous 802.1X sessions:

```
Device(config)# ap dot1x max-sessions 100
```

ap dot1x username

To configure the 802.1X username and password for all access points that are currently joined to the device and any access points that join the device in the future, use the **ap dot1x username** command. To disable the 802.1X username and password for all access points that are currently joined to the device, use the **no** form of this command.

ap dot1x username *user-id* **password** {**0**| **8**} *password-string*

no ap dot1x username *user-id***password** {**0**| **8**} *password-string*

Syntax Description

user-id	Username.
password	Specifies an 802.1X password for all access points.
0	Specifies an unencrypted password.
8	Specifies an AES encrypted password.
password_string	Password.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should 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 words 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:

```
Device(config)# ap dot1x username cisco123 password 0 cisco2020
```

ap ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **ap ethernet duplex** command. To disable the Ethernet port duplex and speed settings of lightweight access points, use the **no** form of this command.

ap ethernet duplex *duplex* **speed** *speed*

no ap ethernet

Syntax Description

duplex	Ethernet port duplex settings. You can specify the following options to configure the duplex settings: • **auto—**Specifies the Ethernet port duplex auto settings. • **half—**Specifies the Ethernet port duplex half settings. • **full—**Specifies the Ethernet port duplex full settings.
speed	Specifies the Ethernet port speed settings.
speed	Ethernet port speed settings. You can specify the following options to configure the speed settings: • **auto—**Specifies the Ethernet port speed to auto. • **10—**Specifies the Ethernet port speed to 10 Mbps. • **100—**Specifies the Ethernet port speed to 100 Mbps. • **1000—**Specifies the Ethernet port speed to 1000 Mbps.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the Ethernet port duplex full settings as 1000 Mbps for all access points:

```
Device(config)# ap ethernet duplex full speed 1000
```

ap group

To create a new access point group, use the **ap group** command. To remove an access point group, use the **no** form of this command.

ap group *group-name*

no ap group *group-name*

Syntax Description

group-name	Access point group name.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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, move all APs in this group to another group. The access points are not moved to the default-group access point group automatically. To see the APs, enter the **show ap summary** command. To move access points, enter the **ap name** *Cisco-AP* **ap-groupname** *Group-Name* command.

This example shows how to create a new access point group:

```
Device(config)# ap group sampleapgroup
```

ap image

To configure an image on all access points that are associated to the device, use the **ap image** command.

ap image {**predownload**| **reset**| **swap**}

Syntax Description

predownload	Instructs all the access points to start predownloading an image.
reset	Instructs all the access points to reboot.
swap	Instructs all the access points to swap the image.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to predownload an image to all access points:

```
Device# ap image predownload
```

This example shows how to reboot all access points:

```
Device# ap image reset
```

This example shows how to swap the access point's primary and secondary images:

```
Device# ap image swap
```

ap ipv6 tcp adjust-mss

To configure IPv6 TCP maximum segment size (MSS) value for all Cisco APs, use the **ap ipv6 tcp adjust-mss** command.

ap ipv6 tcp adjust-mss *size*

no ap ipv6 tcp adjust-mss *size*

Syntax Description

adjust-mss	Configures IPv6 TCP MSS settings for all Cisco APs.
size	MSS value in the range of 500 to 1440.

Command Default

None

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The MSS value must be in the range of 500 to 1440.

This example shows how to configure the IPv6 TCP MSS value to 600 for all Cisco APs:

```
Device(config)# ap ipv6 tcp adjust-mss 600
```

ap led

To enable the LED state for an access point, use the **ap led** command. To disable the LED state for an access point, use the **no** form of this command.

ap led

no ap led

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the LED state for an access point:

```
Device(config)# ap led
```

ap link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for access points, use the **ap link-encryption** command. To disable the DTLS data encryption for access points, use the **no** form of this command.

ap link-encryption

no ap link-encryption

Syntax Description

This command has no keywords and arguments.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable data encryption for all the access points that are joined to the controller:

```
Device(config)# ap link-encryption
```

ap link-latency

To enable link latency for all access points that are currently associated to the device, use the **ap link-latency** command. To disable link latency all access points that are currently associated to the device, use the **no** form of this command.

ap link-latency [**reset**]

no ap link-latency

Syntax Description

reset	(Optional) Resets all link latency for all access points.

Command Default

Link latency is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command enables or disables link latency only for those access points that are currently joined to the device. It does not apply to access points that join in the future.

This example shows how to enable the link latency for all access points:

```
Device(config)# ap link-latency
```

ap mgmtuser username

To configure the username, password, and secret password for access point management, use the **ap mgmtuser username** command.

ap mgmtuser username *username* **password** *password_type password* **secret** *secret_type secret*

Syntax Description

username	Specifies the username for access point management.
password	Specifies the password for access point management.
password_type	Password type. You can specify any one of the following two password types: • **0—**Specifies that an unencrypted password will follow. • **8—**Specifies that an AES encrypted password will follow.
password	Access point management password. **Note** The password does not get encrypted by service-password encryption.
secret	Specifies the secret password for privileged access point management.
secret_type	Secret type. You can specify any one of the following two secret types: • **0—**Specifies that an unencrypted secret password will follow. • **8—**Specifies that an AES encrypted secret password will follow.
secret	Access point management secret password.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To specify a strong password, the following password requirements should be met:

- 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 should not contain a management username or the reverse of a username.
- The password should not contain words such as 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.

To specify a strong secret password, the following requirement should be met:

- The secret password should contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

This example shows how to add a username, password, and secret password for access point management:

```
Device(config)# ap mgmtuser username glbusr password 0 Arc_1234 secret 0 Mid_1234
```

ap name ap-groupname

To add a Cisco lightweight access point to a specific access point group, use the **ap name ap-groupname** command.

ap name *ap-name* **ap-groupname** *group-name*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
group-name	Descriptive name for the access point group.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to add the access point AP01 to the access point group superusers:

```
Device# ap name AP01 ap-groupname superusers
```

ap name antenna band mode

To configure the antenna mode, use the **ap name<AP name> antenna-band-mode{ single | dual }** command.

ap name*ap-name* **antenna-band-mode**{**single**| **dual**}

Syntax Description

ap- name	Name of the Cisco lightweight access point.
antenna-band-mode	Instructs the access point to enable the band mode of antenna.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

This example shows how to configure the antenna band mode of access point.

```
Deviceap name <ap-name> antenna-band-mode single
```

ap name bhrate

To configure the Cisco bridge backhaul Tx rate, use the **ap name bhrate** command.

ap name *ap-name* **bhrate** *kbps*

Syntax Description

ap-name	Name of the Cisco access point.
kbps	Cisco bridge backhaul Tx rate in kbps. The valid values are 6000, 12000, 18000, 24000, 36000, 48000, and 54000.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the Cisco bridge backhaul Tx rate to 54000 kbps:

```
Device# ap name AP02 bhrate 54000
```

ap name bridgegroupname

To set a bridge group name on a Cisco lightweight access point, use the **ap name bridgegroupname** command. To delete a bridge group name on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **bridgegroupname** *bridge_group_name*

ap name *ap-name* **no bridgegroupname**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Only access points with the same bridge group name can connect to each other. Changing the access point bridgegroupname may strand the bridge access point.

This example shows how to set a bridge group name on Cisco access point's bridge group name AP02:

```
Device# ap name AP02 bridgegroupname West
```

This example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
Device# ap name AP02 no bridgegroupname
```

ap name bridging

To enable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **ap name bridging** command. To disable Ethernet-to-Ethernet bridging on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **bridging**

ap name *ap-name* **no bridging**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable Ethernet-to-Ethernet bridging on an access point:

```
Device# ap name TSIM_AP2 bridging
```

ap name cdp interface

To enable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **ap name** command. To disable the Cisco Discovery Protocol (CDP) on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

ap name *ap-name* [**no**] **cdp interface** {**ethernet** *ethernet-id*| **radio** *radio-id*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
ethernet	Enables CDP on an Ethernet interface.
ethernet-id	Ethernet interface number from 0 to 3.
radio	Enables CDP for a radio interface.

radio-id	Radio ID slot number from 0 to 3.

Command Default

Disabled on all access points.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

CDP over Ethernet/radio interfaces is available only when CDP is enabled. After you enable CDP on all access points that are joined to the device, you can disable and then reenable CDP on individual access points by using the **ap name** *ap-name* **cdp interface ethernet** *ethernet-id* cisco_ap command. After you disable CDP on all access points that are joined to the device, you cannot enable and then disable CDP on individual access points.

This example shows how to enable CDP for Ethernet interface number 0 on an access point:

```
Device# ap name TSIM_AP2 cdp interface ethernet 0
```

ap name console-redirect

To redirect the remote debug output of a Cisco lightweight access point to the console, use the **ap name console-redirect** command. To disable the redirection of the remote debug output of a Cisco lightweight access point to the console, use the **no** form of this command.

ap name *ap-name* **console-redirect**

ap name *ap-name* [**no**] **console-redirect**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable redirecting remote debug output of a Cisco access point named AP02 to the console:

```
Device# ap name AP02 console-redirect
```

ap name capwap retransmit

To configure the access point control packet retransmission interval and control packet retransmission count, use the **ap name capwap retransmit** command.

ap name *ap-name* **capwap retransmit** {**count** *count-value*| **interval** *interval-time*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
count	Sets the number of times control packet will be retransmitted.
count-value	Number of times that the control packet will be retransmitted from 3 to 8.
interval	Sets the control packet retransmission timeout interval.
interval-time	Control packet retransmission timeout from 2 to 5 seconds.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the retransmission interval for an access point:

```
Device# ap name AP01 capwap retransmit interval 5
```

This example shows how to configure the retransmission retry count for a specific access point:

```
Device# ap name AP01 capwap retransmit count 5
```

ap name command

To execute a command remotely on a specific Cisco access point, use the **ap name command** command.

ap name *ap-name* **command** "*command* "

Syntax Description

ap-name	Name of the Cisco access point.
command	Command to be executed on a Cisco access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to remotely enter the **show ip interface brief** command on the Cisco access point named TSIM_AP2:

```
Device# ap name AP2 command "show ip interface brief"
```

ap name core-dump

To configure a Cisco lightweight access point's memory core dump, use the **ap name core-dump** command. To disable a Cisco lightweight access point's memory core dump, use the **no** form of this command.

ap name *ap-name* **core-dump** *tftp-ip-addr filename* {**compress**| **uncompress**}

ap name *ap-name* [**no**]**core-dump**

Syntax Description

ap-name	Name of the access point.
tftp-ip-addr	IP address of the TFTP server to which the access point sends core dump files.
filename	Name that the access point used to label the core file.
compress	Compresses the core dump file.

uncompress	Uncompresses the core dump file.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The access point must be able to reach the TFTP server before you can use this command.

This example shows how to configure and compress the core dump file:

```
Device# ap name AP2 core-dump 192.1.1.1 log compress
```

ap name country

To configure the country of operation for a Cisco lightweight access point, use the **ap name country** command.

ap name *ap-name* **country** *country-code*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
country-code	Two-letter or three-letter country code.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Cisco devices 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 to ensure proper unit functionality. See the related product guide for the most recent country codes and regulatory domains. Also, access point regulatory domains are defined during the access point manufacturing process. You can change the access point country code if the new country code matches a country that is valid within the access point regulatory domain. If you try to enter a country that is not valid to the access point regulatory domain, the command fails.

This example shows how to configure the Cisco lightweight access point's country code to DE:

```
Device# ap name AP2 country JP
```

ap name crash-file

To manage crash data and radio core files for the Cisco access point, use the **ap name crash-file** command.

ap name *ap-name* **crash-file** {**get-crash-data**| **get-radio-core-dump** {**slot 0**| **slot 1**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
get-crash-data	Collects the latest crash data for a Cisco lightweight access point.
get-radio-core-dump	Gets a Cisco lightweight access point's radio core dump
slot	Slot ID for Cisco access point.
0	Specifies Slot 0.
1	Specifies Slot 1.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to collect the latest crash data for access point AP3:

```
Device# ap name AP3 crash-file get-crash-data
```

This example shows how to collect the radio core dump for access point AP02 and slot 0:

```
Device# ap name AP02 crash-file get-radio-core-dump slot 0
```

ap name dot11 24ghz rrm coverage

To configure coverage hole detection settings on the 2.4 GHz band, use the **ap name dot11 24ghz rrm coverage** command.

ap name *ap-name* **dot11 24ghz rrm coverage** {**exception** *value*| **level** *value*}

Syntax Description

ap-name	Name of the Cisco access point.
exception	Specifies the percentage of clients on an access point that are experiencing a low signal level but cannot roam to another access point.
value	Percentage of clients. Valid values are from 0 to 100%. **Note** The default is 25%.
level	Specifies the minimum number of clients on an access point with a received signal strength indication (RSSI) value at or below the data or voice RSSI threshold.
value	Minimum number of clients. Valid values are from 1 to 75. **Note** The default is 3.

Command Default

The default for the *exception* parameter is 25% and the default for the *level* parameter is 3.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you enable coverage hole detection, the device 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 **ap dot11 24ghz rrm coverage data packet-count** *count* and **ap dot11 24ghz rrm coverage data fail-percentage** *percentage* commands for a 5-second period, the client is considered to be in a pre-alarm condition. The device 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 **ap dot11 24ghz rrm coverage exception** and **ap dot11 24ghz rrm coverage level** commands over a 90-second period. The device 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.

This example shows how to specify the percentage of clients for an access point 2.4 GHz radio that is experiencing a low signal level:

```
Device# ap name AP2 dot11 24ghz rrm coverage exception 25%
```

This example shows how to specify the minimum number of clients on an 802.11b access point with an RSSI value at or below the RSSI threshold:

```
Device# ap name AP2 dot11 24ghz rrm coverage level 60
```

ap name dot11 49ghz rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point on a 4.9 GHz public safety channel, use the **ap name dot11 49ghz rrm profile** command.

ap name *ap-name* **dot11 49ghz rrm profile** {**clients** *value*| **customize**| **exception** *value*| **foreign** *value*| **level** *value*| **noise** *value*| **throughput** *vaue*| **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
exception *value*	Sets the 802.11a Cisco access point coverage exception level from 0 to100 percent.
foreign	Sets the foreign 802.11 transmitter interference threshold.
value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
level *value*	Sets the 802.11a Cisco access point client minimum exception level from 1 to 75 clients.
noise	Sets the 802.11 foreign noise threshold.

value	802.11 foreign noise threshold from –127 to 0 dBm. **Note** The default is –70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.
value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 49ghz rrm profile clients 75
```

This example shows how to turn performance on profile customization for Cisco lightweight access point AP1 on the 4.9 GHz channel:

```
Device# ap name AP1 dot11 49ghz rrm profile customize
```

This example shows how to set the foreign transmitter interference threshold for AP1 to 0 percent:

```
Device# ap name AP1 dot11 49ghz rrm profile foreign 0
```

This example shows how to set the foreign noise threshold for AP1 to 0 dBm:

```
Device# ap name AP1 dot11 49ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Device# ap name AP1 dot11 49ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Device# ap name AP1 dot11 49ghz rrm profile utilization 100
```

ap name dot11 5ghz rrm channel

To configure a new channel using an 802.11h channel announcement, use the **ap name dot11 5ghz rrm channel** command.

ap name *ap-name* **dot11 5ghz rrm channel** *channel*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
channel	New channel.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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

```
Device# ap name AP01 dot11 5ghz rrm channel 140
```

ap name dot11 antenna

To configure radio antenna settings for Cisco lightweight access points on different 802.11 networks, use the **ap name dot11 antenna** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **antenna** {**ext-ant-gain** *gain*| **mode** {**omni**| **sectorA**| **sectorB**}| **selection** {**external**| **internal**}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.

ext-ant-gain	Specifies the external antenna gain for an 802.11 network. **Note** Before you enter this command, disable the Cisco radio by using the **ap dot11** {**24ghz** | **5ghz**} **shutdown** command. After you enter this command, reenable the Cisco radio by using the **no ap dot11** {**24ghz** | **5ghz**} **shutdown** command.
gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).
mode	Specifies that the Cisco lightweight access point is 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.
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.
selection	Selects the internal or external antenna selection for a Cisco lightweight access point on an 802.11 network.
external	Specifies the external antenna.
internal	Specifies the internal antenna.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a 5 GHz external antenna gain of 0.5 dBm for AP1:

```
Device# ap name AP1 dot11 5ghz antenna ext-ant-gain 0.5
```

This example shows how to configure access point AP01 antennas for a 360-degree omnidirectional pattern on a 2.4 GHz band:

```
Device# ap name AP01 dot11 24ghz antenna mode omni
```

This example shows how to configure access point AP02 on a 2.4 GHz band to use the internal antenna:

```
Device# ap name AP02 dot11 24ghz antenna selection interval
```

ap name dot11 antenna extantgain

To configure radio antenna settings for Cisco lightweight access points on 4.9 GHz and 5.8 GHz public safety channels, use the **ap name dot11 antenna extantgain** command.

ap name *ap-name* **dot11** {**49ghz**| **58ghz**} {**antenna extantgain** *gain*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
49ghz	Specifies 4.9 GHz public safety channel settings.
58ghz	Specifies 5.8 GHz public safety channel settings.
gain	Antenna gain in 0.5 dBm units (for example, 2.5 dBm = 5).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you enter this command, disable the Cisco radio by using the **ap dot11** {**24ghz | 5ghz**} **shutdown** command. After you enter this command, reenable the Cisco radio by using the **no ap dot11** {**24ghz | 5ghz**} **shutdown** command.

This example shows how to configure an external antenna gain of 0.5 dBm for AP1 on a 4.9 GHz public safety channel:

```
Device# ap name AP1 dot11 49ghz antenna extantgain 0.5
```

ap name dot11 cleanair

To configure CleanAir settings for a specific Cisco lightweight access point on 802.11 networks, use the **ap name dot11 cleanair** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.

Command Default

Disabled.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable CleanAir on the 2.4 GHz band:

```
Device# ap name AP01 dot11 24ghz cleanair
```

ap name dot11 dot11n antenna

To configure an access point to use a specific antenna, use the **ap name dot11 dot11n antenna** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **dot11n antenna** {**A**| **B**| **C**| **D**}

Syntax Description

ap-name	Access point name.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
A	Specifies antenna port A.
B	Specifies antenna port B.
C	Specifies antenna port C.
D	Specifies antenna port D.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable antenna B on access point AP02:

```
Device# ap name AP02 dot11 5ghz dot11n antenna B
```

This example shows how to disable antenna C on access point AP02:

```
Device# ap name AP02 no dot11 5ghz dot11n C
```

ap name dot11 dual-band cleanair

To configure CleanAir for a dual band radio, use the **ap name dot11 dual-band cleanair** command.

ap name *ap-name* **dot11 dual-band cleanair**

ap name *ap-name* **no dot11 dual-band cleanair**

Syntax Description

ap-name	Name of the Cisco AP.
cleanair	Specifies the CleanAir feature.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This example shows how to enable CleanAir for a dual band radio of the access point AP01:

```
Device# ap name AP01 dot11 dual-band cleanair
```

ap name dot11 dual-band shutdown

To disable dual band radio on a Cisco AP, use the **ap name dot11 dual-band shutdown** command.

ap name *ap-name* **dot11 dual-band shutdown**

ap name *ap-name* **no dot11 dual-band shutdown**

Syntax Description

ap-name	Name of the Cisco AP.
shutdown	Disables the dual band radio on the Cisco AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This example shows how to disable dual band radio on the Cisco access point AP01:

```
Device# ap name AP01 dot11 dual-band shutdown
```

ap name dot11 rrm ccx

To configure Cisco Client eXtension (CCX) Radio Resource Management (RRM) settings for specific Cisco lightweight access points on 802.11 networks, use the **ap name dot11 rrm ccx** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm ccx** {**customize**| **location-measurement** *interval*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
customize	Enables 802.11 CCX options.
location-measurement	Configures the CCX client location measurements.

interval	Interval from 10 to 32400.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure CCX client location measurements for an access point in the 2.4 GHz band:

```
Device# ap name AP01 dot11 24ghz rrm ccx location-measurement 3200
```

ap name dot11 rrm profile

To configure Radio Resource Management (RRM) performance profile settings for a Cisco lightweight access point, use the **ap name dot11 rrm profile** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **rrm profile** {**clients** *value*| **customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
clients	Sets the access point client threshold.
value	Access point client threshold from 1 to 75 clients. **Note** The default client threshold is 12.
customize	Turns on performance profile customization for an access point. **Note** Performance profile customization is off by default.
foreign	Sets the foreign 802.11 transmitter interference threshold.

value	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. **Note** The default is 10 percent.
noise	Sets the 802.11 foreign noise threshold.
value	802.11 foreign noise threshold between –127 and 0 dBm. **Note** The default is —70 dBm.
throughput	Sets the data-rate throughput threshold.
value	802.11 throughput threshold from 1000 to 10000000 bytes per second. **Note** The default is 1,000,000 bytes per second.
utilization	Sets the RF utilization threshold. **Note** The operating system generates a trap when this threshold is exceeded.
value	802.11 RF utilization threshold from 0 to 100 percent. **Note** The default is 80 percent.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the AP1 clients threshold to 75 clients:

```
Device# ap name AP1 dot11 24ghz rrm profile clients 75
```

This example shows how to turn performance profile customization on for 802.11a Cisco lightweight access point AP1:

```
Device# ap name AP1 dot11 5ghz rrm profile customize
```

This example shows how to set the foreign 802.11a transmitter interference threshold for AP1 to 0 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile foreign 0
```

This example shows how to set the 802.11a foreign noise threshold for AP1 to 0 dBm:

```
Device# ap name AP1 dot11 5ghz rrm profile noise 0
```

This example shows how to set the AP1 data-rate threshold to 10000000 bytes per second:

```
Device# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Device# ap name AP1 dot11 5ghz rrm profile utilization 100
```

ap name dot11 txpower

To configure the transmit power level for a single access point in an 802.11 network, use the **ap name dot11 txpower** command.

ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**shutdown**| **txpower** {**auto**| *power-level*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
shutdown	Disables the 802.11 networks.
auto	Specifies the power level is automatically set by Radio Resource Management (RRM) for the 802.11 Cisco radio.
power-level	Manual transmit power level number for the access point.

Command Default

The command default (txpower auto) is for automatic configuration by RRM.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to automatically set the 2.4 GHz radio transmit power for access point AP1:

```
Device# ap name AP1 dot11 24ghz txpower auto
```

ap name dot1x-user

To configure the global authentication username and password for an access point that is currently joined to the device, use the **ap name dot1x-user** command. To disable 802.1X authentication for a specific access point, use the **no** form of this command.

ap name *ap-name* **dot1x-user** {**global-override**| **username** *user-id* **password** *passwd*}

ap name *ap-name* [**no**] **dot1x-user**

Syntax Description

ap-name	Name of the access point.
global-override	Forces the access point to use the device's global authentication settings.
username	Specifies to add a username.
user-id	Username.
password	Specifies to add a password.
passwd	Password.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should 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 words in any language.

  You can set the values for a specific access point.

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.

This example shows how to configure a specific username and password for dot1x authentication:

```
Device# ap name AP02 dot1x-user username Cisco123 password Cisco2020
```

This example shows how to disable the authentication for access point cisco_ap1:

```
Device# ap name cisco_ap1 no dot1x-user
```

ap name ethernet

To configure ethernet port settings of a Cisco lightweight access point, use the **ap name ethernet** command. To remove configured port settings or set of defaults, use the **no** form of this command.

ap name *ap-name* **ethernet** *intf-number* **mode** {**access** *vlan-id*| **trunk** [**add**| **delete**]} **native-vlan** *vlan-id*

ap name *ap-name* **no ethernet** *intf-number* **mode** {**access**| **trunk native-vlan**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
intf-number	Ethernet interface number from 0 to 3.
mode	Configures access or trunk mode.
access	Configures the port in access mode.
vlan-id	VLAN identifier.
trunk	Specifies the port in trunk mode.
add	(Optional) Adds a VLAN or trunk mode.
delete	(Optional) Deletes a VLAN or trunk mode.
native-vlan	Specifies a native VLAN.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure access mode for a Cisco access point.

```
Device# ap name AP2 ethernet 0 mode access 1
```

ap name ethernet duplex

To configure the Ethernet port duplex and speed settings of the lightweight access points, use the **ap name ethernet duplex** command.

ap name *ap-name* **ethernet duplex** {**auto**| **full**| **half**} **speed**{**10**| **100**| **1000**| **auto**}

Syntax Description

ap-name	Name of the Cisco access point.
auto	Specifies the Ethernet port duplex auto settings.
full	Specifies the Ethernet port duplex full settings.
half	Specifies the Ethernet port duplex half settings.
speed	Specifies the Ethernet port speed settings.
10	Specifies the Ethernet port speed to 10 Mbps.
100	Specifies the Ethernet port speed to 100 Mbps.
1000	Specifies the Ethernet port speed to 1000 Mbps.
auto	Specifies the Ethernet port setting for all connected access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the Ethernet port to full duplex and 1 Gbps for an access point:

```
Device# ap name AP2 ethernet duplex full 1000
```

ap name key-zeroize

To enable the FIPS key-zeroization on an Access Point, use the **ap name<AP name> key-zeroize**command.

ap name*ap-name* **key-zeroize**

Syntax Description

ap- name	Name of the Cisco lightweight access point.
key-zeroize	Instructs the access point to enable the FIPS key-zeroization on AP.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

This example shows how to enable FIPS key-zeroization.

```
Deviceap name <AP Name> key-zeroize
```

ap name image

To configure an image on a specific access point, use the **ap name image** command.

ap name *ap-name* **image** {**predownload**| **swap**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
predownload	Instructs the access point to start the image predownload.
swap	Instructs the access point to swap the image.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to predownload an image to an access point:

```
Device# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Device# ap name AP2 image swap
```

ap name ipv6 tcp adjust-mss

To configure IPv6 TCP maximum segment size (MSS) value for a Cisco AP, use the **ap name ipv6 tcp adjust-mss** command.

ap name *ap-name* **ipv6 tcp adjust-mss** *size*

ap name *ap-name* **no ipv6 tcp adjust-mss**

Syntax Description

ap-name	Name of the Cisco AP.
adjust-mss	Configures IPv6 TCP MSS settings for all Cisco APs.
size	MSS value in the range of 500 to 1440.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

The MSS value must be in the range of 500 to 1440.

This example shows how to configure the IPv6 TCP MSS value to 600 for a Cisco access point AP01:

```
Device# ap name AP01 ipv6 tcp adjust-mss 600
```

ap name jumbo mtu

To configure the Jumbo MTU support, use the **ap name<AP name>jumbo-mtu**command.

ap name*ap-name* {**jumbo-mtu**| **no jumbo-mtu**}

Syntax Description

ap- name	Name of the Cisco lightweight access point.
jumbo-mtu	Instructs the access point to enable the Jumbo MTU support.
no jumbo-mtu	Instructs the access point to disable the Jumbo MTU support.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

This example shows how to configure the Jumbo MTU support.

```
Deviceap name <AP Name> jumbo-mtu
```

ap name lan

To configure LAN port configurations for APs, use the **ap name lan** command. To remove LAN port configurations for APs, use the**ap name no lan** command.

ap name *ap-name* **[no]lan port-id** *port-id* {**shutdown**|**vlan-access**}

Syntax Description

no	Removes LAN port configurations.
port-id	Configures the port.
port-id	The ID of the port. The range is 1-4

shotdown	Disables the Port.
vlan-access	Enables VLAN access to Port.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to enable VLAN access to port:

```
Device# ap name AP1 lan port-id 1 vlan-access
```

ap name led

To enable the LED state for an access point, use the **ap name led** command. To disable the LED state for an access point, use the **no** form of this command.

ap name *ap-name* **led**

no ap name *ap-name* [**led**] **led**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
led	Enables the access point's LED state.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the LED state for an access point:

```
Device# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Device# ap name AP2 no led
```

ap name link-encryption

To enable Datagram Transport Layer Security (DTLS) data encryption for specific Cisco lightweight access points, use the **ap name link-encryption** command. To disable DTLS data encryption for specific Cisco lightweight access points, use the **no** form of this command.

ap name *ap-name* **link-encryption**

ap name *ap-name* **no link-encryption**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable data encryption for an access point:

```
Device# ap name AP02 link-encryption
```

ap name link-latency

To enable link latency for a specific Cisco lightweight access point that is currently associated to the device, use the **ap name link-latency** command. To disable link latency for a specific Cisco lightweight access point that is currently associated to the device, use the **no** form of this command.

ap name *ap-name* **link-latency**

ap name *ap-name* **no link-latency**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

Link latency is disabled by default.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command enables or disables link latency only for access points that are currently joined to the device. It does not apply to access points that join in the future.

This example shows how to enable link latency on access points:

```
Device# ap name AP2 link-latency
```

ap name location

To modify the descriptive location of a Cisco lightweight access point, use the **ap name location** command.

ap name *ap-name* **location** *location*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
location	Location name of the access point (enclosed by double quotation marks).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point must be disabled before changing this parameter.

This example shows how to configure the descriptive location for access point AP1:

```
Device# ap name AP1 location Building1
```

ap name mgmtuser

To configure the username, password, and secret password for access point management, use the **ap name mgmtuser** command. To force a specific access point to use the device's global credentials, use the **no** form of this command.

ap name *ap-name* **mgmtuser username** *username* **password** *password* **secret** *secret*

ap name *ap-name* **no mgmtuser**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
username	Specifies the username for access point management.
username	Management username.
password	Specifies the password for access point management.
password	Access point management password.
secret	Specifies the secret password for privileged access point management.
secret	Access point management secret password.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To specify a strong password, you should adhere to the following requirements:

- 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 cannot contain a management username or the reverse of a username.
- The password cannot contain words such as 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 cannot contain characters from at least three of the following classes: lowercase letters, uppercase letters, digits, or special characters.

This example shows how to add a username, password, and secret password for access point management:

```
Device# ap name AP01 mgmtuser username acd password Arc_1234 secret Mid_1234
```

ap name mode

To change a Cisco device communication option for an individual Cisco lightweight access point, use the **ap name mode** command.

ap name *ap-name* **mode**{**local submode**{**none**| **wips**}| **monitor submode**{**none**| **wips**}| **rogue**| **se-connect**| **sniffer**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
local	Converts from an indoor mesh access point (MAP or RAP) to a nonmesh lightweight access point (local mode).
submode	Specifies wIPS submode on an access point.
none	Disables the wIPS on an access point.
monitor	Specifies monitor mode settings.
wips	Enables the wIPS submode on an access point.
rogue	Enables wired rogue detector mode on an access point.
se-connect	Enables spectrum expert mode on an access point.
sniffer	Enables wireless sniffer mode on an access point.

Command Default

Local

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

This example shows how to set the device to communicate with access point AP01 in local mode:

```
Device# ap name AP01 mode local submode none
```

This example shows how to set the device to communicate with access point AP01 in a wired rogue access point detector mode:

```
Device# ap name AP01 mode rogue
```

This example shows how to set the device to communicate with access point AP02 in wireless sniffer mode:

```
Device# ap name AP02 mode sniffer
```

ap name monitor-mode

To configure Cisco lightweight access point channel optimization, use the **ap name monitor-mode** command.

ap name *ap-name* **monitor-mode** {**no-optimization**| **tracking-opt**| **wips-optimized**}

Syntax Description

ap-name	Name of the Cisco lightweight 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.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a Cisco wireless intrusion prevention system (wIPS) monitor mode on access point AP01:

```
Device# ap name AP01 monitor-mode wips
```

ap name monitor-mode dot11b

To configures 802.11b scanning channels for a monitor-mode access point, use the **ap name monitor-mode dot11b** command.

ap name *ap-name* **monitor-mode dot11b fast-channel** *channel1* [*channel2*] [*channel3*] [*channel4*]

Syntax Description

ap-name	Name of the access point.
fast-channel	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
channel1	Scanning channel1.
channel2	(Optional) Scanning channel2.
channel3	(Optional) Scanning channel3.
channel4	(Optional) Scanning channel4.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure an access point in tracking optimized mode to listen to channels 1, 6, and 11:

```
Device# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

ap name name

To modify the name of a Cisco lightweight access point, use the **ap name name** command.

ap name *ap-name* **name** *new-name*

Syntax Description

ap-name	Current Cisco lightweight access point name.
new-name	Desired Cisco lightweight access point name.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to modify the name of access point AP1 to AP2:

```
Device# ap name AP1 name AP2
```

ap name no dot11 shutdown

To enable radio transmission for an individual Cisco radio on an 802.11 network, use the **ap name no dot11 shutdown** command.

ap name *ap-name* **no dot11** {**24ghz**| **5ghz**} **shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz radios.
5ghz	Specifies the 5 GHz radios.

Command Default

The transmission is enabled for the entire network by default.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Note Use this command with the **ap name** *Cisco-AP* **dot11 5ghz shutdown** command when configuring 802.11 settings.

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

This example shows how to enable radio transmission on the 5 GHz band for access point AP1:

```
Device# ap name AP1 no dot11 5ghz shutdown
```

ap name power

To enable the Cisco Power over Ethernet (PoE) feature for access points, use the **ap name power** command. To disable the Cisco PoE feature for access points, use the **no** form of this command.

ap name *ap-name* **power** {**injector**| **pre-standard**}

ap name *ap-name* **no power** {**injector**| **pre-standard**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
injector	Specifies the power injector state for an access point.
pre-standard	Enables the inline power Cisco prestandard switch state for an access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the power injector state for all access points:

```
Device# ap name AP01 power injector
```

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Device# ap name AP02 power pre-standard
```

ap name shutdown

To disable a Cisco lightweight access point, use the **ap name shutdown** command. To enable a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **shutdown**

ap name *ap-name* **no shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example how to disable a specific Cisco lightweight access point:

```
Device# ap name AP2 shutdown
```

ap name slot shutdown

To disable a slot on a Cisco lightweight access point, use the **ap name slot shutdown** command. To enable a slot on a Cisco lightweight access point, use the **no** form of the command.

ap name *ap-name* **slot** {**0**| **1**| **2**| **3**} **shutdown**

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

0	Enables slot number 0 on a Cisco lightweight access point.
1	Enables slot number 1 on a Cisco lightweight access point.
2	Enables slot number 2 on a Cisco lightweight access point.
3	Enables slot number 3 on a Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable slot 0 on a Cisco access point named TSIM_AP2:

```
Device# ap name TSIM_AP2 no slot 0 shutdown
```

ap name sniff

To enable sniffing on an access point, use the **ap name sniff** command. To disable sniffing on an access point, use the **no** form of this command.

ap name *ap-name* **sniff** {**dot11a**| **dot11b**}

ap name *ap-name* **no sniff** {**dot11a**| **dot11b**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot11a	Specifies the 2.4 GHz band.
dot11b	Specifies the 5 GHz band.
channel	Valid channel to be sniffed. For the 5 GHz band, the range is 36 to 165. For the 2.4 GHz band, the range is 1 to 14.
server-ip-address	IP address of the remote machine running Omnipeek, Airopeek, AirMagnet, or Wireshark software.

Command Default

Channel 36

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 about 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 that are sent by the access point.

This example shows how to enable the sniffing on the 5 GHz band for an access point on the primary wireless LAN controller:

```
Device# ap name AP2 sniff dot11a 36 192.0.2.54
```

ap name ssh

To enable Secure Shell (SSH) connectivity on a specific Cisco lightweight access point, use the **ap name ssh** command. To disable SSH connectivity on a specific Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **ssh**

ap name *ap-name* **no ssh**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The Cisco lightweight access point associates with this Cisco device for all network operations and in the event of a hardware reset.

This example shows how to enable SSH connectivity on access point Cisco_ap2:

```
Device# ap name Cisco_ap2 ssh
```

ap name telnet

To enable Telnet connectivity on an access point, use the **ap name telnet** command. To disable Telnet connectivity on an access point, use the **no** form of this command.

ap name *ap-name* **telnet**

ap name *ap-name* **no telnet**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable Telnet connectivity on access point cisco_ap1:

```
Device# ap name cisco_ap1 no telnet
```

ap name power injector

To configure the power injector state for an access point, use the **ap name power injector** command. To disable the Cisco Power over Ethernet (PoE) feature for access points, use the **no** form of this command.

ap name *ap-name* **power injector** {**installed**| **override**| **switch-mac-address** *switch-MAC-address*}

ap name *ap-name* **no power injector**

Syntax Description

ap-name	Name of he Cisco lightweight access point.
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-address	Specifies the MAC address of the switch port with an installed power injector.
switch-MAC-address	MAC address of the switch port with an installed power injector.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the power injector state for an access point:

```
Device# ap name AP01 power injector switch-mac-address aaaa.bbbb.cccc
```

ap name power pre-standard

To enable the inline power Cisco prestandard switch state for an access point, use the **ap name power pre-standard** command. To disable the inline power Cisco prestandard switch state for an access point, use the **no** form of this command.

ap name *ap-name* **power pre-standard**

ap name *ap-name* **no power pre-standard**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Device# ap name AP02 power pre-standard
```

This example shows how to disable the inline power Cisco prestandard switch state for access point AP02:

```
Device# ap name AP02 no power pre-standard
```

ap name reset-button

To configure the Reset button for an access point, use the **ap name reset-button** command.

ap name *ap-name* **reset-button**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the Reset button for access point AP03:

```
Device# ap name AP03 reset-button
```

ap name reset

To reset a specific Cisco lightweight access point, use the **ap name reset** command.

ap name *ap-name* **reset**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to reset a Cisco lightweight access point named AP2:

```
Device# ap name AP2 reset
```

ap name slot

To configure various slot parameters, use the **ap name slot** command. To disable a slot on a Cisco lightweight access point, use the **no** form of this command.

ap name *ap-name* **slot** *slot-number* {**channel** {**global**| **number** *channel-number*| **width** *channel-width*}| **rtsthreshold** *value*| **shutdown**| **txpower** {**global**| *channel-level*}}

ap name *ap-name* **no slot** {**0**| **1**| **2**| **3**} **shutdown**

Syntax Description

ap-name	Name of the Cisco access point.
slot-number	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: • **0—**Enables slot number 0 on a Cisco lightweight access point. • **1—**Enables slot number 1 on a Cisco lightweight access point. • **2—**Enables slot number 2 on a Cisco lightweight access point. • **3—**Enables slot number 3 on a Cisco lightweight access point.
channel	Specifies the channel for the slot.
global	Specifies channel global properties for the slot.
number	Specifies the channel number for the slot.

channel-number	Channel number from 1 to 169.
width	Specifies the channel width for the slot.
channel-width	Channel width from 20 to 40.
rtsthreshold	Specifies the RTS/CTS threshold for an access point.
value	RTS/CTS threshold value from 0 to 65535.
shutdown	Shuts down the slot.
txpower	Specifies Tx power for the slot.
global	Specifies auto-RF for the slot.
channel-level	Transmit power level for the slot from 1 to 7.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable slot 3 for the access point abc:

```
Device# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Device# ap name abc slot 3 rtsthreshold 54
```

ap name static-ip

To configure lightweight access point static IP settings, use the **ap name static-ip** command. To disable the Cisco lightweight access point static IP address, use the **no** form of this command.

ap name *ap-name* **static-ip** {**domain** *domain-name*| **ip-address** *ip-address* **netmask** *netmask* **gateway** *gateway*| **nameserver** *ip-address*}

ap name *ap-name* **no static-ip**

Syntax Description

ap-name	Name of the access point.

domain	Specifies the Cisco access point domain name.
domain-name	Domain to which a specific access point belongs.
ip-address	Specifies the Cisco access point static IP address.
ip-address	Cisco access point static IP address.
netmask	Specifies the Cisco access point static IP netmask.
netmask	Cisco access point static IP netmask.
gateway	Specifies the Cisco access point gateway.
gateway	IP address of the Cisco access point gateway.
nameserver	Specifies a DNS server so that a specific access point can discover the device using DNS resolution.
ip-address	IP address of the DNS server.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

An access point cannot discover the device 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.

This example shows how to configure an access point static IP address:

```
Device# ap name AP2 static-ip ip-address 192.0.2.54 netmask 255.255.255.0 gateway 192.0.2.1
```

ap name stats-timer

To set the time in seconds that the Cisco lightweight access point sends its DOT11 statistics to the Cisco device, use the **ap name stats-timer** command.

ap name *ap-name* **stats-timer** *timer-value*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
timer-value	Time in seconds from 0 to 65535. A zero value disables the timer.

Command Default

0 (Disabled).

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

This example shows how to set the stats timer to 600 seconds for access point AP2:

```
Device# ap name AP2 stats-timer 600
```

ap name syslog host

To configure a syslog server for a specific Cisco lightweight access point, use the **ap name syslog host** command.

ap name *ap-name* **syslog host** *syslog-host-ip-address*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
syslog-host-ip-address	IP address of the syslog server.

Command Default

255.255.255.255

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the syslog server IP address for each access point is 255.255.255.255, which indicates 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 example shows how to configure a syslog server:

```
Device# ap name AP2 syslog host 192.0.2.54
```

ap name syslog level

To configure the system logging level, use the **ap name syslog level** command.

ap name *ap-name* **syslog level** {**alert**| **critical**| **debug**| **emergency**| **errors**| **information**| **notification**| **warning**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
alert	Specifies alert level system logging.
critical	Specifies critical level system logging.
debug	Specifies debug level system logging.
emergency	Specifies emergency level system logging.
errors	Specifies error level system logging.
information	Specifies information level system logging.
notification	Specifies notification level system logging.
warning	Specifies warning level system logging.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure alert level system logging:

```
Device# ap name AP2 syslog level alert
```

ap name tcp-adjust-mss

To enable or disable the TCP maximum segment size (MSS) on a particular access point, use the **ap name tcp-adjust-mss** command. To disable the TCP maximum segment size (MSS) on a particular access point, use the **no** form of this command.

ap name *ap-name* **tcp-adjust-mss size** *size*

ap name *ap-name* **no tcp-adjust-mss**

Syntax Description

ap-name	Name of the access point.
size	Maximum segment size, from 536 to 1363 bytes.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, the access point changes the MSS to the new configured value. If the MSS of these packets is greater than the value that you have configured or greater than the default value for the CAPWAP tunnel, the access point changes the MSS to the newly configured value.

This example shows how to enable the TCP MSS on access point Cisco_ap1:

```
Device# ap name ciscoap tcp-adjust-mss size 1200
```

ap name tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap name tftp-downgrade** command.

ap name *ap-name* **tftp-downgrade** *tftp-server-ip filename*

Syntax Description

ap-name	Name of the Cisco lightweight access point.
tftp-server-ip	IP address of the TFTP server.
filename	Filename of the access point image file on the TFTP server.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the settings for downgrading access point AP1:

```
Device# ap name Ap01 tftp-downgrade 172.21.12.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

ap power injector

To configure the power injector state for all the Cisco lightweight access points that are joined to the device, use the **ap power injector** command. To delete the power injector state for all access points, use the **no** form of this command.

ap power injector {**installed**| **override**| **switch-mac-address** *switch-MAC-addr*}

no ap power injector

Syntax Description

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-address	Specifies the MAC address of the switch port with an installed power injector.
switch-MAC-address	Specifies the MAC address of the switch port with an installed power injector.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the power injector state for all the Cisco lightweight access points that are joined to the device:

```
Device(config)# ap power injector switch-mac-address aaaa.bbbb.cccc
```

ap power pre-standard

To set the Cisco lightweight access points that are joined to the device to be powered by a high-power Cisco switch, use the **ap power pre-standard** command. To disable the pre standard power for all access points, use the **no** form of this command.

ap power pre-standard

no ap power pre-standard

Syntax Description

This command has no keywords and arguments.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Controller(config)# ap power pre-standard
```

ap reporting-period

To configure the access point rogue/error reporting period, use the **ap reporting-period** command. To disable the access point rogue/error reporting period, use the **no** form of this command.

ap reporting-period *value*

no ap reporting-period

Syntax Description

value	Time period in seconds from 10 to 120.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example show how to configure the access point rogue/error reporting:

```
Device(config)# ap reporting-period 100
```

This example show how to disable the access point rogue/error reporting:

```
Device(config)# no ap reporting-period 100
```

ap reset-button

To configure the Reset button for all Cisco lightweight access points that are joined to the device, use the **ap reset-button** command. To disable the Reset button for all access points, use the **no** form of this command.

ap reset-button

no ap reset-button

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the Reset button for all access points that are joined to the controller:

```
Device(config)# ap reset-button
```

service-policy type control subscriber

To apply the global subscriber control policy, use the **service-policy type control subscriber** *<subscriber-policy-name>*command.

service-policytypecontrolsubscriber*<subscriber-policy-name>*

Syntax Description

service-policy	Instructs the access point to apply global subscriber control policy.
<subscriber-policy-name>	Name of the subscriber policy.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

This example shows how to disable the global subscriber control policy.

```
Deviceno service-policy type control subscriber
```

ap static-ip

To configure Cisco lightweight access point static IP address settings, use the **ap static-ip** command. To disable access point static IP settings, use the **no** form of this command.

ap static-ip {**domain** *domain-name*| **name-server** *ip-address*}

no ap static-ip {**domain**| **name-server**}

Syntax Description

domain	Specifies the domain to which a specific access point or all access points belong.
domain-name	Domain name.
name-server	Specifies a DNS server so that a specific access point or all access points can discover the device using DNS resolution.
ip-address	DNS server IP address.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

An access point cannot discover the device 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.

This example shows how to configure a static IP address for all access points:

```
Device(config)# ap static-ip domain cisco.com
```

ap syslog

To configure the system logging settings for all Cisco lightweight access points that are joined to the device, use the **ap syslog** command.

ap syslog {**host** *ipaddress*| **level**{**alert**| **critical**| **debug**| **emergency**| **errors**| **information**| **notification**| **warning**}}

Syntax Description

host	Specifies a global syslog server for all access points that join the device.
ipaddress	IP address of the syslog server.
level	Specifies the system logging level for all the access points joined to the device.
alert	Specifies alert level system logging for all Cisco access points.
critical	Specifies critical level system logging for all Cisco access points.
debug	Specifies debug level system logging for all Cisco access points.
emergency	Specifies emergency level system logging for all Cisco access points.
errors	Specifies errors level system logging for all Cisco access points.
information	Specifies information level system logging for all Cisco access points.
notification	Specifies notification level system logging for all Cisco access points.
warning	Specifies warning level system logging for all Cisco access points.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 device. If the access points cannot reach this subnet, the access points are unable to send out syslog messages.

This example shows how to configure a global syslog server for all access points:

```
Device(config)# ap syslog host 172.21.34.45
```

ap name no controller

To change the order of configured primary, secondary and tertiary wireless LAN controllers use the following commands.

ap name*ap-name* **no controller primary**

ap name*ap-name* **no controller secondary**

ap name*ap-name* **no controller tertiary**

Syntax Description

ap- name	Name of the Cisco lightweight access point.
no controller primary	Instructs the access point to unconfigure the primary controller.
no controller secondary	Instructs the access point to unconfigure the secondary controller.
no controller tertiary	Instructs the access point to unconfigure the tertiary controller.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

If you have the primary, secondary, and tertiary wireless LAN controllers configured for an access point and you require swap the controller names and the corresponding IP addresses you can uncofigure the primary and configure the secondary controller.

Example

This example shows how to unconfigure the primary controller.

```
Deviceap name <AP Name> no controller primary.
```

ap tcp-adjust-mss size

To enable the TCP maximum segment size (MSS) on all Cisco lightweight access points, use the **ap tcp-adjust-mss size** command. To disable the TCP maximum segment size (MSS) on all Cisco lightweight access points **no** form of this command.

ap tcp-adjust-mss size *size*

no ap tcp-adjust-mss

Syntax Description

size	Maximum segment size, from 536 to 1363 bytes.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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 Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, the access point changes the MSS to the new configured value.

This example shows how to enable the TCP MSS on all access points with a segment size of 1200:

```
Device(config)# ap tcp-adjust-mss 1200
```

ap tftp-downgrade

To configure the settings used for downgrading a lightweight access point to an autonomous access point, use the **ap tftp-downgrade** command. To disable the settings used for downgrading a lightweight access point to an autonomous access point, use the **no** form of this command.

ap tftp-downgrade *tftp-server-ip filename*

no ap tftp-downgrade

Syntax Description

tftp-server-ip	IP address of the TFTP server.

filename	Filename of the access point image file on the TFTP server.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the settings for downgrading all access points:

```
Device(config)# ap tftp-downgrade 172.21.23.45 ap3g1-k9w7-tar.124-25d.JA.tar
```

config wireless wps rogue client mse

To configure a rogue MSE client, use **wirelesswps rogueclientmse**command.

To view the summary of the wireless client statistics, use **show wirelessclientclient-statisticssummary** command.

wirelesswpsrogueclientmse

showwirelessclientclient-statisticssummary

Syntax Description

rogueclient mse	Instructs the access point to enable configuring a rogue MSE client.
nowireless wps	Instructs the access point to disable the configuring a rogue MSE client.
client-statisticssummary	Instructs to view the summary of the wireless client statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

This example shows how to configure a rogue MSE client.

```
Devicewireless wps rogue client mse
```

clear ap name tsm dot11 all

To clear the traffic stream metrics (TSM) statistics for a particular access point or all the access points, use the **clear ap name tsm dot11 all** command.

clear ap name *ap-name* **tsm dot11** {**24ghz**| **5ghz**} **all**

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
all	Specifies all access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to clear the TSM statistics for an access point on the 2.4 GHz band:

```
Device# clear ap name AP1 tsm dot11 24ghz all
```

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* [**eventlog**| **keep-ip-config**]

Syntax Description

ap-name	Name of the Cisco lightweight access point.
eventlog	(Optional) Deletes the existing event log and creates an empty event log file for a specific access point or for all access points joined to the device.
keep-ip-config	(Optional) Specifies not to erase the static IP configuration of the Cisco access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

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

This example shows how to clear the access point's configuration settings for the access point named AP01:

```
Device# clear ap config AP01
```

clear ap eventlog-all

To delete the existing event log and create an empty event log file for all access points, use the **clear ap eventlog-all** command.

clear ap eventlog-all

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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

```
Device# clear ap eventlog-all
```

clear ap join statistics

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

clear ap join statistics

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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

```
Device# clear ap join statistics
```

clear ap mac-address

To clear the MAC address for the join statistics for a specific Cisco lightweight access point, use the **clear ap mac-address** command.

clear ap mac-address *mac* **join statistics**

Syntax Description

mac	Access point MAC address.
join statistics	Clears join statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to clear the join statistics of an access point:

```
Device# clear ap mac-address aaaa.bbbb.cccc join statistics
```

clear ap name wlan statistics

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

clear ap name *ap-name* **wlan statistics**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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

```
Device# clear ap name cisco_ap wlan statistics
```

debug ap mac-address

To enable debugging of access point on the mac-address, use the **debug ap mac-address** command.

debug ap mac-address *mac-address*

no debug ap mac-address *mac-address*

Syntax Description

mac-address	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
10.3Cisco IOS XE 3.3 SE	This command was introduced.

This example shows how to enable debugging mac-address on an AP :

```
Device# debug ap mac-address
ap mac-address debugging is on
```

This example shows how to disable debugging mac-address on an AP :

```
Device# no debug ap mac-address
ap mac-address debugging is off
```

show ap cac voice

To display the list of all access points with brief voice statistics, which include bandwidth used, maximum bandwidth available, and the call information, use the **show ap cac voice** command.

show ap cac voice

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display voice CAC details that correspond to Cisco lightweight access points:

```
controller# show ap cac voice

1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ----------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ---------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0


2) AP Name: AP02
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ----------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ---------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0
```

show ap capwap

To display the Control and Provisioning of Wireless Access Points (CAPWAP) configuration that is applied to all access points, use the **show ap capwap** command.

show ap capwap {**retransmit**| **timers**| **summary**}

Syntax Description

retransmit	Displays the access point CAPWAP retransmit parameters.
timers	Displays the rogue access point entry timers.
summary	Displays the network configuration of the Cisco device.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the access point CAPWAP retransmit parameters:

```
Controller# show ap capwap retransmit

Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval            Retransmit Count
--------------------------------------------------------------------------------
AP01                              3                               5

AP02                              3                               5

AP03                              3                               5

AP04                              3                               5

AP05                              3                               5

AP07                              3                               5

AP08                              3                               5

AP09                              3                               5

AP10                              3                               5

AP11                              3                               5

AP12                              3                               5
```

This example shows how to display the rogue access point entry timers:

```
Controller# show ap capwap timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
```

```
Fast Heartbeat timeout   : 1
```

This example shows how to display the the network configuration of the Cisco device:

```
Controller# show ap capwap summary

AP Fallback                      : Enabled
AP Join Priority                 : Disabled
AP Master                        : Disabled
Primary backup Controller Name   :
Primary backup Controller IP     : 0.0.0.0
Secondary backup Controller Name :
Secondary backup Controller IP   : 0.0.0.0
```

show ap cdp

To display the Cisco Discovery Protocol (CDP) information for all Cisco lightweight access points that are joined to the device, use the **show ap cdp** command.

show ap cdp [**neighbors** [**detail**]]

Syntax Description

neighbors	(Optional) Displays neighbors using CDP.
detail	(Optional) Displays details about a specific access point neighbor that is using CDP.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the CDP status of all access points:

```
Device# show ap cdp
```

This example shows how to display details about all neighbors that are using CDP:

```
Device# show ap cdp neighbors
```

show ap config dot11

To display the detailed configuration of 802.11-58G radios on Cisco lightweight access points, use the **show ap config dot11** command.

show ap config dot11 58ghz summary

Syntax Description

58ghz	Displays the 802.11-58G radios.
summary	Displays a summary of the radios on the access points.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the detailed configuration of 802.11a-58G radios on access points:

```
Device# show ap config dot11 58ghz summary
```

show ap config dot11 dual-band summary

To view a summary of configuration settings for dual band radios of Cisco APs, use the **show ap config dot11 dual-band summary** command.

show ap config dot11 dual-band summary

Syntax Description

dual-band	Specifies the dual band radio.
summary	Displays a summary of configuration settings for dual band radios of Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

show ap config fnf

To view Netflow input and output monitors for all Cisco APs, use the **show ap config fnf** command.

show ap config fnf

Syntax Description

fnf	Netflow input and output monitors for all Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

show ap config

To display configuration settings for all access points that join the device, use the **show ap config** command.

show ap config {**ethernet**| **general**| **global**}

Syntax Description

ethernet	Displays ethernet VLAN tagging information for all Cisco APs.
general	Displays common information for all Cisco APs.
global	Displays global settings for all Cisco APs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display global syslog server settings:

```
Device# show ap config global
AP global system logging host                    : 255.255.255.255
```

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 keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the crash file generated by the access point:

```
Device# show ap crash-file
```

show ap data-plane

To display the data plane status, use the **show ap data-plane** command.

show ap data-plane

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example show how to display the data plane status for all access points:

```
Device# show ap data-plane
```

show ap dot11 l2roam

To display 802.11a or 802.11b/g Layer 2 client roaming information, use the **show ap dot11 l2roam** command.

show ap dot11 {**24ghz**| **5ghz**} **l2roam** {**mac-address** *mac-address* **statistics**| **rf-param**| **statistics**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
mac-address *mac-address* **statistics**	Specifies the MAC address of a Cisco lightweight access point.
rf-param	Specifies the Layer 2 frequency parameters.
statistics	Specifies the Layer 2 client roaming statistics.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display 802.11b Layer 2 client roaming information:

```
Device# show ap dot11 24ghz l2roam rf-param

L2Roam 802.11bg RF Parameters
  Config Mode          : Default
  Minimum RSSI         : -85
  Roam Hysteresis      : 2
  Scan Threshold       : -72
  Transition time      : 5
```

show ap dot11 cleanair air-quality

To display the air-quality summary information and air-quality worst information for the 802.11 networks, use the **show ap dot11 cleanair air-quality** command.

show ap dot11 {**24ghz**| **5ghz**} **cleanair air-quality** {**summary**| **worst**}

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
summary	Displays a summary of 802.11 radio band air-quality information.
worst	Displays the worst air-quality information for 802.11 networks.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the worst air-quality information for the 5 GHz band:

```
Device# show ap dot11 5ghz cleanair air-quality worst

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel Avg AQ Min AQ Interferers DFS
------------ ------- ------ ------ ----------- -----
CISCO_AP3500 36      95     70     0           40
```

This example shows how to display the worst air-quality information for the 2.4 GHz band:

```
Device# show ap dot11 24ghz 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 ap dot11 cleanair config

To display the CleanAir configuration for the 802.11 networks, use the **show ap dot11 cleanair config** command.

show ap dot11 {**24ghz**| **5ghz**} **cleanair config**

Syntax Description

24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the CleanAir configuration for the 2.4 GHz band:

```
Device# show ap dot11 24ghz cleanair config
Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
    Interference Device Reporting................. : Enabled
        Bluetooth Link............................ : Enabled
        Microwave Oven............................ : Enabled
        802.11 FH................................. : Enabled
        Bluetooth Discovery....................... : Enabled
        TDD Transmitter........................... : Enabled
        Jammer.................................... : Enabled
        Continuous Transmitter.................... : Enabled
        DECT-like Phone........................... : Enabled
        Video Camera.............................. : Enabled
        802.15.4.................................. : Enabled
        WiFi Inverted............................. : Enabled
        WiFi Invalid Channel...................... : Enabled
        SuperAG................................... : Enabled
        Canopy.................................... : Enabled
        Microsoft Device.......................... : Enabled
        WiMax Mobile.............................. : Enabled
        WiMax Fixed............................... : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link............................ : Disabled
```

```
        Microwave Oven........................... : Disabled
        802.11 FH................................ : Disabled
        Bluetooth Discovery...................... : Disabled
        TDD Transmitter.......................... : Disabled
        Jammer................................... : Disabled
        Continuous Transmitter................... : Disabled
        DECT-like Phone.......................... : Disabled
        Video Camera............................. : Disabled
        802.15.4................................. : Disabled
        WiFi Inverted............................ : Enabled
        WiFi Invalid Channel..................... : Enabled
        SuperAG.................................. : Disabled
        Canopy................................... : Disabled
        Microsoft Device......................... : Disabled
        WiMax Mobile............................. : Disabled
        WiMax Fixed.............................. : Disabled
    Interference Device Alarms................... : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State.............. : Disabled
    CleanAir Driven RRM Sensitivity.............. : LOW
    CleanAir Persistent Devices state............ : Disabled
```

show ap dot11 cleanair summary

To view CleanAir configurations for all 802.11a Cisco APs, use the **show ap dot11 cleanair summary** command.

show ap dot11 {**24ghz**| **5ghz**} **cleanair summary**

Syntax Description

24ghz	Specifies the 2.4-GHz band
5ghz	Specifies the 5-GHz band
cleanair summary	Summary of CleanAir configurations for all 802.11a Cisco APs

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

show ap dot11

To view 802.11a or 802.11b configuration information, use the **show ap dot11** command.

show ap dot11 {**24ghz**| **5ghz**} {**channel**| **coverage**| **group**| **load-info**| **logging**| **media-stream**| **monitor**| **network**| **profile**| **receiver**| **service-policy**| **summary**| **txpower**| **ccx global**}

Syntax Description

24ghz	Specifies the 2.4 GHz band.
5ghz	Specifies the 5 GHz band.
channel	Displays the automatic channel assignment configuration and statistics.
coverage	Displays the configuration and statistics for coverage hole detection.
group	Displays 802.11a or 802.11b Cisco radio RF grouping.
load-info	Displays channel utilization and client count information for all Cisco APs.
logging	Displays 802.11a or 802.11b RF event and performance logging.
media-stream	Display 802.11a or 802.11b Media Resource Reservation Control configurations.
monitor	Displays the 802.11a or 802.11b default Cisco radio monitoring.
network	Displays the 802.11a or 802.11b network configuration.
profile	Displays the 802.11a or 802.11b lightweight access point performance profiles.
receiver	Displays the configuration and statistics of the 802.11a or 802.11b receiver.
service-policy	Displays the Quality of Service (QoS) service policies for 802.11a or 802.11b radio for all Cisco access points.
summary	Displays the 802.11a or 802.11b Cisco lightweight access point name, channel, and transmit level summary.
txpower	Displays the 802.11a or 802.11b automatic transmit power assignment.
ccx global	Displays 802.11a or 802.11b Cisco Client eXtensions (CCX) information for all Cisco access points that are joined to the device.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **load-info** parameter was added.

This example shows how to display the automatic channel assignment configuration and statistics:

```
Device# show ap dot11 5ghz channel
Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 12 Hours
  Anchor time (Hour of the day)              : 20
  Channel Update Contribution                : SNI.
  Channel Assignment Leader                  : web (9.9.9.2)
  Last Run                                   : 13105 seconds ago
  DCA Sensitivity Level                      : MEDIUM (15 dB)
  DCA 802.11n Channel Width                  : 40 Mhz
  Channel Energy Levels
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  Channel Dwell Times
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                       : 36,40,44,48,52,56,60,64,149,153,1
57,161
  Unused Channel List                        : 100,104,108,112,116,132,136,140,1
65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                       :
  Unused Channel List                        : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,
15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                      : Disabled
```

This example shows how to display the statistics for coverage hole detection:

```
Device# show ap dot11 5ghz coverage
Coverage Hole Detection
  802.11a Coverage Hole Detection Mode          : Enabled
  802.11a Coverage Voice Packet Count           : 100 packet(s)
  802.11a Coverage Voice Packet Percentage      : 50 %
  802.11a Coverage Voice RSSI Threshold         : -80dBm
  802.11a Coverage Data Packet Count            : 50 packet(s)
  802.11a Coverage Data Packet Percentage       : 50 %
  802.11a Coverage Data RSSI Threshold          : -80dBm
  802.11a Global coverage exception level       : 25
  802.11a Global client minimum exception level   : 3 clients
```

This example shows how to display Cisco radio RF group settings:

```
Device# show ap dot11 5ghz group
Radio RF Grouping

  802.11a Group Mode                 : STATIC
```

```
  802.11a Group Update Interval      : 600 seconds
  802.11a Group Leader               : web (10.10.10.1)
  802.11a Group Member               : web(10.10.10.1)
                                       nb1(172.13.21.45) (*Unreachable)
  802.11a Last Run                   : 438 seconds ago


  Mobility Agents RF membership information
  ------------------------------------------------------------
  No of 802.11a MA RF-members : 0
```

This example shows how to display 802.11a RF event and performance logging:

```
Device# show ap dot11 5ghz 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
```

This example shows how to display the 802.11a media stream configuration:

```
Device# show ap dot11 5ghz media-stream
Multicast-direct                 : Disabled
Best Effort                      : Disabled
Video Re-Direct                  : Disabled
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 (Kbps)               : 6000
Max Retry Percentage              : 80
```

This example shows how to display the radio monitoring for the 802.11b network:

```
Device# show ap dot11 5ghz monitor
Default 802.11a AP monitoring

  802.11a Monitor Mode                          : Enabled
  802.11a Monitor Mode for Mesh AP Backhaul     : disabled
  802.11a Monitor Channels                      : Country channels
  802.11a RRM Neighbor Discover Type            : Transparent
  802.11a AP Coverage Interval                  : 180 seconds
  802.11a AP Load Interval                      : 60 seconds
  802.11a AP Noise Interval                     : 180 seconds
  802.11a AP Signal Strength Interval           : 60 seconds
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz profile
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
```

This example shows how to display the network configuration of an 802.11a profile:

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled
```

```
802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
```

```
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz receiver
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
```

This example shows how to display the global configuration and statistics of an 802.11a profile:

```
Device# show ap dot11 5ghz service-policy
```

This example shows how to display a summary of the 802.11b access point settings:

```
Device# show ap dot11 5ghz 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(*)
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz txpower
Automatic Transmit Power Assignment

Transmit Power Assignment Mode          : AUTO
Transmit Power Update Interval          : 600 seconds
Transmit Power Threshold                : -70 dBm
Transmit Power Neighbor Count           : 3 APs
Min Transmit Power                      : -10 dBm
Max Transmit Power                      : 30 dBm
Transmit Power Update Contribution      : SNI.
Transmit Power Assignment Leader        : web (10.10.10.1)
Last Run                                : 437 seconds ago
```

This example shows how to display the configuration and statistics of the 802.11a transmit power cost:

```
Device# show ap dot11 5ghz ccx global
 802.11a Client Beacon Measurements:
     disabled
```

show ap env summary

To show ap environment summary, use the **show ap env summary** command.

There is no keyword or argument.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show ap environment summary:

```
Device#show ap env summary
```

show ap ethernet statistics

To display Ethernet statistics for all Cisco lightweight access points, use the **show ap ethernet statistics** command.

show ap ethernet statistics

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display Ethernet statistics for all access points:

```
Device# show ap ethernet statistics
```

show ap gps-location summary

To show GPS location summary of all connected Cisco APs, use the **show ap gps-location summary** command.

There is no keyword or argument.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show GPS location summary of all connected Cisco APs:

```
Device# show ap gps-location summary
```

show ap groups

To display information about all access point groups that are defined in the system, use the **show ap groups** command.

show ap groups

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display information about all access point groups:

```
Device# show ap groups
```

show ap groups extended

To view information about all AP groups defined in the system in detail, use the **show ap groups extended** command.

show ap groups extended

Syntax Description

extended	Displays information about all AP groups defined in the system in detail.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

show ap image

To display the images present on Cisco lightweight access points, use the **show ap image** command.

show ap image

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display images on the access points:

```
Device# show ap image
```

show ap is-supported

To see if an AP model is supported or not, use the **show ap is-supported** command.

show ap is-supported *model-part-number*

Syntax Description

model-part-number	Part number of the AP model. For example, AIR-LAP1142N-N-K9.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.7.0E	This command was introduced.

This example shows how to check if an AP model is supported or not:

```
Device# show ap is-supported AIR-LAP1142N-N-K9
AP Support: Yes
```

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

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To obtain the MAC address of the 802.11 radio interface, enter the **show interface** command on the access point.

This example shows how to display specific join information for an access point:

```
Device# show ap join stats summary
Number of APs : 1

Base MAC        Ethernet MAC    AP Name                IP Address       Status

--------------- --------------- --------------------- --------------- -------------
-
c8f9.f91a.aa80  0000.0000.0000  N A                   0.0.0.0          Not Joined
```

show ap link-encryption

To display the link encryption status, use the **show ap link-encryption** command.

show ap link-encryption

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example show how to display the link-encryption status:

```
Device# show ap link-encryption
```

show ap mac-address

To display join-related statistics collected and last join error details for access points, use the **show ap mac-address** command.

show ap mac-address *mac-address* **join stats** {**detailed**| **summary**}

Syntax Description

mac-address	Access point Ethernet MAC address or the MAC address of the 802.11 radio interface.
join stats	Displays join information and statistics for Cisco access points.

detailed	Displays all join-related statistics collected.
summary	Displays the last join error detail.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display join information for a specific access point that is trying to join the device:

```
Device# show ap mac-address d0c2.8267.8b00 join stats detailed

Discovery phase statistics
  Discovery requests received                              : 6
  Successful discovery responses sent                      : 6
  Unsuccessful discovery request processing                : 0
  Reason for last unsuccessful discovery attempt           : Not applicable
  Time at last successful discovery attempt                : Nov 20 17:25:10.841
  Time at last unsuccessful discovery attempt              : Not applicable

Join phase statistics
  Join requests received                                   : 3
  Successful join responses sent                           : 3
  Unsuccessful join request processing                     : 0
  Reason for last unsuccessful join attempt                : Not applicable
  Time at last successful join attempt                     : Nov 20 17:25:20.998
  Time at last unsuccessful join attempt                   : Not applicable

Configuration phase statistics
  Configuration requests received                          : 8
  Successful configuration responses sent                  : 3
  Unsuccessful configuration request processing            : 0
  Reason for last unsuccessful configuration attempt       : Not applicable
  Time at last successful configuration attempt            : Nov 20 17:25:21.177
  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                   : Number of message retransmission
 to the AP has reached maximum

Last join error summary
  Type of error that occurred last                         : AP got or has been disconnected

  Reason for error that occurred last                     : Number of message retransmission
 to the AP has reached maximum
  Time at which the last join error occurred               : Nov 20 17:22:36.438
```

This example shows how to display specific join information for an access point:

```
Device# show ap mac-address d0c2.8267.8b00 join stats detailed

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 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 keywords and arguments.	

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display current channel-optimized monitor mode settings:

```
Device# 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 name auto-rf

To display the auto-RF settings for a Cisco lightweight access point, use the **show ap name auto-rf** command.

show ap name *ap-name* **auto-rf dot11** {**24ghz**| **5ghz**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default None

Command Modes Privileged EXEC.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display auto-RF information for an access point:

```
Device# show ap name AP01 auto-rf dot11 24ghz

Number of Slots                                  : 2
AP Name                                          : TSIM_AP-1
MAC Address                                      : 0000.2000.02f0
Slot ID                                          : 0
Radio Type                                       : 802.11b/g
Subband Type                                     : All

Noise Information
  Noise Profile                                  : Failed
  Channel   1                                     :   24 dBm
  Channel   2                                     :   48 dBm
  Channel   3                                     :   72 dBm
  Channel   4                                     :   96 dBm
  Channel   5                                     :  120 dBm
  Channel   6                                     : -112 dBm
  Channel   7                                     :  -88 dBm
  Channel   8                                     :  -64 dBm
  Channel   9                                     :  -40 dBm
  Channel  10                                     :  -16 dBm
  Channel  11                                     :    8 dBm

Interference Information
  Interference Profile                           : Passed
  Channel   1                                     : -128 dBm @  0% busy
  Channel   2                                     :  -71 dBm @  1% busy
  Channel   3                                     :  -72 dBm @  1% busy
  Channel   4                                     :  -73 dBm @  2% busy
  Channel   5                                     :  -74 dBm @  3% busy
  Channel   6                                     :  -75 dBm @  4% busy
  Channel   7                                     :  -76 dBm @  5% busy
  Channel   8                                     :  -77 dBm @  5% busy
  Channel   9                                     :  -78 dBm @  6% busy
  Channel  10                                     :  -79 dBm @  7% busy
  Channel  11                                     :  -80 dBm @  8% busy

Rogue Histogram (20/40_ABOVE/40_BELOW)
    Channel  36                                   : 27/ 4/ 0
    Channel  40                                   : 13/ 0/ 0
    Channel  44                                   :  5/ 0/ 0
    Channel  48                                   :  6/ 0/ 1
    Channel  52                                   :  4/ 0/ 0
    Channel  56                                   :  5/ 0/ 0
    Channel  60                                   :  1/ 3/ 0
    Channel  64                                   :  3/ 0/ 0
    Channel 100                                   :  0/ 0/ 0
    Channel 104                                   :  0/ 0/ 0
    Channel 108                                   :  0/ 1/ 0

Load Information
  Load Profile                                   : Passed
```

```
  Receive Utilization                            : 10%
  Transmit Utilization                           : 20%
  Channel Utilization                            : 50%
  Attached Clients                               : 0 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 dB                                    : 0 clients
  SNR    5 dB                                    : 0 clients
  SNR   10 dB                                    : 0 clients
  SNR   15 dB                                    : 0 clients
  SNR   20 dB                                    : 0 clients
  SNR   25 dB                                    : 0 clients
  SNR   30 dB                                    : 0 clients
  SNR   35 dB                                    : 0 clients
  SNR   40 dB                                    : 0 clients
  SNR   45 dB                                    : 0 clients

Nearby APs
  AP 0000.2000.0300 slot 0                       : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0400 slot 0                       : -68 dBm on  11 (10.10.10.1)
  AP 0000.2000.0600 slot 0                       : -68 dBm on  11 (10.10.10.1)

Radar Information

Channel Assignment Information
  Current Channel Average Energy                 : 0 dBm
  Previous Channel Average Energy                : 0 dBm
  Channel Change Count                           : 0
  Last Channel Change Time                       : Wed Oct 17 08:13:36 2012
  Recommended Best Channel                       : 11

RF Parameter Recommendations
  Power Level                                    : 1
  RTS/CTS Threshold                              : 2347
  Fragmentation Threshold                        : 2346
  Antenna Pattern                                : 0

Persistent Interference Devices
```

show ap name bhmode

To display Cisco bridge backhaul mode, use the **show ap name bhmode** command.

show ap name *ap-name* **bhmode**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display Cisco bridge backhaul mode of an access point:

```
Device# show ap name TSIM_AP-1 bhmode
```

show ap name bhrate

To display the Cisco bridge backhaul rate, use the **show ap name bhrate** command.

show ap name *ap-name* **bhrate**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the Cisco bridge backhaul rate for an access point:

```
Device# show ap name AP01 bhrate
```

show ap name cac voice

To display voice call admission control details for a specific Cisco lightweight access point, use the **show ap name cac voice** command.

show ap name *ap-name* **cac voice**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display voice call admission control details for an access point:

```
Device# show ap name AP01 cac voice
1) AP Name: AP01
============================

  Wireless Bandwidth (In MeanTime mt)

       Slot#  Radio         Calls  BW-Max  BW-Alloc  Bw-InUse (%age)
  ----------------------------------------------------------------
  1    0      802.11b/g     0      23437   0         0
  2    1      802.11a       0      23437   0         0

  Wired Bandwidth (in Kbps)

       Slot#  Wlan-ID  Wlan-Name             BW-Config   BW-Avail
  ---------------------------------------------------------------
  1    0      1        maria-open            0           0
  2    0      12       24                    0           0
  3    1      1        maria-open            0           0
  4    1      12       24                    0           0
```

show ap name config fnf

To view the Netflow input and output monitors for a Cisco AP, use the **show ap name config fnf** command.

show ap name *ap-name* **config fnf**

Syntax Description

ap-name	Name of the Cisco lightweight access point
fnf	Netflow input and output monitors for a Cisco AP

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

show ap name dot11 call-control

To display call control information and the metrics for successful calls, use the **show ap name dot11 call-control** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **call-control** {**call-info**| **metrics**}

Syntax Description

ap-name	Name of the Cisco lightweight access point
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
call-info	Displays call information.
metrics	Displays call metrics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display metrics for successful calls for an access point:

```
Device# show ap name AP01 dot11 24ghz call-control metrics

Slot#   Call Count      Call Duration
--------------------------------
0       0               0
```

show ap name cable-modem

To show AP CAPWAP CCX on a specific AP, use the **show ap name cable-modem**command.

show ap name *ap-name***cable-modem**

Syntax Description

ap-name	Name of the specific AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show AP CAPWAP CCX on AP1:

```
Device# show ap name ap1 cable-modem
```

show ap name capwap retransmit

To display Control and Provisioning of Wireless Access Points (CAPWAP) retransmit settings, use the **show ap name capwap retransmit** command.

show ap name *ap-name* **capwap retransmit**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CAPWAP retransmit settings of an access point:

```
Device# show ap name AP01 capwap retransmit

AP Name   Retransmit Interval Retransmit Count
--------  ------------------- ----------------
AP01      3                   5
```

show ap name ccx rm

To display an access point's Cisco Client eXtensions (CCX) radio management status information, use the **show ap name ccx rm** command.

show ap name *ap-name* **ccx rm status**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CCX radio management information for an access point:

```
Device# show ap name AP01 ccx rm status

802.11b/g Radio
  Beacon Request                                  : Disabled
  Channel Load Request                            : Disabled
  Frame Request                                   : Disabled
  Noise Histogram Request                         : Disabled
  Path Loss Request                               : Disabled
  Interval                                        : 60
  Iteration                                       : 0

802.11a Radio
  Beacon Request                                  : Disabled
  Channel Load Request                            : Disabled
  Frame Request                                   : Disabled
  Noise Histogram Request                         : Disabled
  Path Loss Request                               : Disabled
  Interval                                        : 60
  Iteration                                       : 0
```

show ap name cdp

To display the Cisco Discovery Protocol (CDP) information for an access point, use the **show ap name cdp** command.

show ap name *ap-name* **cdp** [**neighbors** [**detail**]]

Syntax Description

ap-name	Name of the Cisco lightweight access point.
neighbors	(Optional) Displays neighbors that are using CDP.
detail	(Optional) Displays details about a specific access point neighbor that is using CDP.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CDP information for an access point:

```
Device# show ap name AP01 cdp neighbors detail
```

show ap name channel

To display the available channels for a specific mesh access point, use the **show ap name channel** command.

show ap name *ap-name* **channel**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the available channels for a particular access point:

```
Device# show ap name AP01 channel

Slot ID                                          : 0
Allowed Channel List                             : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                   10, 11
Slot ID                                          : 1
Allowed Channel List                             : 36, 40, 44, 48, 52, 56, 60, 64, 100
                                                   104, 108, 112, 116, 132, 136, 140, 149,
 153
                                                   157, 161
```

show ap name config

To display common information and Ethernet VLAN tagging information for a specific Cisco lightweight access point, use the **show ap name config** command.

show ap name *ap-name* **config** {**ethernet**| **general**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
ethernet	Displays Ethernet tagging configuration information for an access point.
general	Displays common information for an access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display Ethernet tagging information for an access point:

```
Device# show ap name AP01 config ethernet

VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Device# show ap name AP01 config general

Cisco AP Name                                   : AP01
Cisco AP Identifier                             : 5
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                            : Unconfigured
Switch Port Number                              : Te1/0/1
MAC Address                                     : 0000.2000.02f0
IP Address Configuration                        : Static IP assigned
IP Address                                      : 10.10.10.12
IP Netmask                                      : 255.255.0.0
Gateway IP Address                              : 10.10.10.1
Fallback IP Address Being Used                  : 10.10.10.12
Domain                                          : Cisco
Name Server                                     : 0.0.0.0
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Enabled
SSH State                                       : Disabled
Cisco AP Location                               : sanjose
Cisco AP Group Name                             : default-group
Primary Cisco Controller Name                   : CAPWAP Controller
Primary Cisco Controller IP Address             : 10.10.10.1
Secondary Cisco Controller Name                 :
Secondary Cisco Controller IP Address           : Not Configured
Tertiary Cisco Controller Name                  :
Tertiary Cisco Controller IP Address            : Not Configured
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : Local
AP Submode                                      : Not Configured
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : informational
Software Version                                : 7.4.0.5
Boot Version                                    : 7.4.0.5
Stats Reporting Period                          : 180
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : Power Injector/Normal Mode
Number of Slots                                 : 2
AP Model                                        : 1140AG
AP Image                                        : C1140-K9W8-M
IOS Version                                     :
Reset Button                                    :
AP Serial Number                                : SIM1140K001
AP Certificate Type                             : Manufacture Installed
Management Frame Protection Validation          : Disabled
AP User Mode                                    : Customized
AP User Name                                    : cisco
AP 802.1X User Mode                             : Not Configured
AP 802.1X User Name                             : Not Configured
Cisco AP System Logging Host                    : 255.255.255.255
AP Up Time                                      : 15 days 16 hours 19 minutes 57
 seconds
AP CAPWAP Up Time                               : 4 minutes 56 seconds
Join Date and Time                              : 10/18/2012 04:48:56
Join Taken Time                                 : 15 days 16 hours 15 minutes 0
seconds
Join Priority                                   : 1
Ethernet Port Duplex                            : Auto
Ethernet Port Speed                             : Auto
AP Link Latency                                 : Disabled
Rogue Detection                                 : Disabled
AP TCP MSS Adjust                               : Disabled
AP TCP MSS Size                                 : 6146
```

show ap name config dot11

To display 802.11 configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name config dot11** command.

show ap name *ap-name* **config dot11** {**24ghz**| **49ghz**| **58ghz**| **5hgz**| **dual-band**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
49ghz	Displays 802.11-4.9G network settings.
58ghz	Displays 802.11-5.8G network settings.
5hgz	Displays the 5 GHz band settings.
dual-band	Displays the dual band radio settings.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **dual-band** parameter was added.

This example shows how to display 802.11b configuration information that corresponds to a specific Cisco lightweight access point:

```
Device# show ap name AP01 config dot11 24ghz

Cisco AP Identifier                              : 5
Cisco AP Name                                    : AP01
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                             : -A
Switch Port Number                               : Te1/0/1
MAC Address                                      : 0000.2000.02f0
IP Address Configuration                         : Static IP assigned
IP Address                                       : 10.10.10.12
IP Netmask                                       : 255.255.0.0
Gateway IP Address                               : 10.10.10.1
Fallback IP Address Being Used                   : 10.10.10.12
Domain                                           : Cisco
```

```
Name Server                                       : 0.0.0.0
CAPWAP Path MTU                                   : 1485
Telnet State                                      : Enabled
SSH State                                         : Disabled
Cisco AP Location                                 : sanjose
Cisco AP Group Name                               : default-group
Administrative State                              : Enabled
Operation State                                   : Registered
AP Mode                                           : Local
AP Submode                                        : Not Configured
Remote AP Debug                                   : Disabled
Logging Trap Severity Level                       : informational
Software Version                                  : 7.4.0.5
Boot Version                                      : 7.4.0.5
Mini IOS Version                                  : 3.0.51.0
Stats Reporting Period                            : 180
LED State                                         : Enabled
PoE Pre-Standard Switch                           : Disabled
PoE Power Injector MAC Address                    : Disabled
Power Type/Mode                                   : Power Injector/Normal Mode
Number of Slots                                   : 2
AP Model                                          : 1140AG
AP Image                                          : C1140-K9W8-M
IOS Version                                       :
Reset Button                                      :
AP Serial Number                                  : SIM1140K001
AP Certificate Type                               : Manufacture Installed
Management Frame Protection Validation            : Disabled
AP User Mode                                      : Customized
AP User Name                                      : cisco
AP 802.1X User Mode                               : Not Configured
AP 802.1X User Name                               : Not Configured
Cisco AP System Logging Host                      : 255.255.255.255
AP Up Time                                        : 15 days 17 hours 9 minutes 41
seconds
AP CAPWAP Up Time                                 : 54 minutes 40 seconds
Join Date and Time                                : 10/18/2012 04:48:56
Join Taken Time                                   : 15 days 16 hours 15 minutes 0
seconds

Attributes for Slot 0
  Radio Type                                      : 802.11n - 2.4 GHz
  Administrative State                            : Enabled
  Operation State                                 : Up
  Cell ID                                         : 0

  Station Configuration
    Configuration                                 : Automatic
    Number of WLANs                               : 1
    Medium Occupancy Limit                        : 100
    CFP Period                                    : 4
    CFP Maximum Duration                          : 60
    BSSID                                         : 000020000200

    Operation Rate Set
       1000 Kbps                                  : MANDATORY
       2000 Kbps                                  : MANDATORY
       5500 Kbps                                  : MANDATORY
      11000 Kbps                                  : MANDATORY
       6000 Kbps                                  : SUPPORTED
       9000 Kbps                                  : SUPPORTED
      12000 Kbps                                  : SUPPORTED
      18000 Kbps                                  : SUPPORTED
      24000 Kbps                                  : SUPPORTED
      36000 Kbps                                  : SUPPORTED
      48000 Kbps                                  : SUPPORTED
      54000 Kbps                                  : 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
    MCS 16                                    : DISABLED
    MCS 17                                    : DISABLED
    MCS 18                                    : DISABLED
    MCS 19                                    : DISABLED
    MCS 20                                    : DISABLED
    MCS 21                                    : DISABLED
    MCS 22                                    : DISABLED
    MCS 23                                    : DISABLED

  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 Channel                               : 0
  Number of Channels                          : 0
  Country String                              : US

MAC Operation Parameters
  Configuration                               : Automatic
  Fragmentation Threshold                     : 2346
  Packet Retry Limit                          : 64
  Legacy Tx Beamforming Setting               : Disabled

Tx Power
  Number of Supported Power Levels            : 8
  Tx Power Level 1                            : 20 dBm
  Tx Power Level 2                            : 17 dBm
  Tx Power Level 3                            : 14 dBm
  Tx Power Level 4                            : 11 dBm
  Tx Power Level 5                            : 8 dBm
  Tx Power Level 6                            : 5 dBm
  Tx Power Level 7                            : 2 dBm
  Tx Power Level 8                            : -1 dBm
  Tx Power Configuration                      : Automatic
  Current Tx Power Level                      : 1

Phy OFDM Parameters
  Configuration                               : Automatic
  Current Channel                             : 11
  Extension Channel                           : None
  Channel Width                               : 20 MHz
  Allowed Channel List                        : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                10, 11
  TI Threshold                                : 0
  Antenna Type                                : Internal
  Internal Antenna Gain (in .5 dBi units)     : 0
  Diversity                                   : Diversity enabled

  802.11n Antennas
    Tx                                        : A, B, C
    Rx                                        : A, B, C

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                       : 15 dB
    Coverage Exception Level                     : 25%
    Client Minimum Exception Level               : 3 clients
    RTS/CTS Threshold                              : 2347
    Short Retry Limit                              : 7
    Long Retry Limit                               : 4
    Max Tx MSDU Lifetime                           : 512
    Max Rx Lifetime                                : 512

  CleanAir Management Information
    CleanAir Capable                             : Yes
    CleanAir Management Admin State              : Enabled
    CleanAir Management Operation State          : Up
    Rapid Udpate Mode                            : Disabled
    Spectrum Expert connection                   : Disabled
    CleanAir NSI Key                             : 377313C8F290E246E640C4EF177BED
88
    Spectrum Expert connections counter          : 0
    CleanAir Sensor State                        : Configured

  Rogue Containment Information
    Containment Count                            : 0
```

show ap name config slot

To display configuration information for slots on a specific Cisco lightweight access point, use the **show ap name config slot** command.

show ap name *ap-name* **config slot** {**0**| **1**| **2**| **3**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
0	Displays slot number 0.
1	Displays slot number 1.
2	Displays slot number 2.
3	Displays slot number 3.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display configuration information for slots on an access point:

```
Device# show ap name AP01 config slot 0

Cisco AP Identifier                              : 3
Cisco AP Name                                    : AP01
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                             : -A
Switch Port Number                               : Te1/0/1
MAC Address                                      : 0000.2000.02f0
IP Address Configuration                         : Static IP assigned
IP Address                                       : 10.10.10.12
IP Netmask                                       : 255.255.0.0
Gateway IP Address                               : 10.10.10.1
Fallback IP Address Being Used                   : 10.10.10.12
Domain                                           : Cisco
Name Server                                      : 0.0.0.0
CAPWAP Path MTU                                  : 1485
Telnet State                                     : Enabled
SSH State                                        : Disabled
Cisco AP Location                                : sanjose
Cisco AP Group Name                              : default-group
Administrative State                             : Enabled
Operation State                                  : Registered
AP Mode                                          : Local
AP Submode                                       : Not Configured
Remote AP Debug                                  : Disabled
Logging Trap Severity Level                      : informational
Software Version                                 : 7.4.0.5
Boot Version                                     : 7.4.0.5
Mini IOS Version                                 : 3.0.51.0
Stats Reporting Period                           : 180
LED State                                        : Enabled
PoE Pre-Standard Switch                          : Disabled
PoE Power Injector MAC Address                   : Disabled
Power Type/Mode                                  : Power Injector/Normal Mode
Number of Slots                                  : 2
AP Model                                         : 1140AG
AP Image                                         : C1140-K9W8-M
IOS Version                                      :
Reset Button                                     :
AP Serial Number                                 : SIM1140K001
AP Certificate Type                              : Manufacture Installed
Management Frame Protection Validation           : Disabled
AP User Mode                                     : Customized
AP User Name                                     : cisco
AP 802.1X User Mode                              : Not Configured
AP 802.1X User Name                              : Not Configured
Cisco AP System Logging Host                     : 255.255.255.255
AP Up Time                                       : 15 days 16 hours 1 minute 19 s
econds
AP CAPWAP Up Time                                : 20 hours 21 minutes 37 seconds

Join Date and Time                               : 10/17/2012 08:13:36
Join Taken Time                                  : 14 days 19 hours 39 minutes 41
 seconds

Attributes for Slot 0
  Radio Type                                     : 802.11n - 2.4 GHz
  Administrative State                           : Enabled
  Operation State                                : Up
  Cell ID                                        : 0

  Station Configuration
    Configuration                                : Automatic
    Number of WLANs                              : 1
    Medium Occupancy Limit                       : 100
    CFP Period                                   : 4
    CFP Maximum Duration                         : 60
    BSSID                                        : 000020000200
```

```
  Operation Rate Set
     1000 Kbps                                 : MANDATORY
     2000 Kbps                                 : MANDATORY
     5500 Kbps                                 : MANDATORY
    11000 Kbps                                 : MANDATORY
     6000 Kbps                                 : SUPPORTED
     9000 Kbps                                 : SUPPORTED
    12000 Kbps                                 : SUPPORTED
    18000 Kbps                                 : SUPPORTED
    24000 Kbps                                 : SUPPORTED
    36000 Kbps                                 : SUPPORTED
    48000 Kbps                                 : SUPPORTED
    54000 Kbps                                 : 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
    MCS 16                                     : DISABLED
    MCS 17                                     : DISABLED
    MCS 18                                     : DISABLED
    MCS 19                                     : DISABLED
    MCS 20                                     : DISABLED
    MCS 21                                     : DISABLED
    MCS 22                                     : DISABLED
    MCS 23                                     : DISABLED

  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 Channel                                : 0
  Number of Channels                           : 0
  Country String                               : US

MAC Operation Parameters
  Configuration                                : Automatic
  Fragmentation Threshold                      : 2346
  Packet Retry Limit                           : 64

Tx Power
  Number of Supported Power Levels             : 8
  Tx Power Level 1                             : 20 dBm
  Tx Power Level 2                             : 17 dBm
  Tx Power Level 3                             : 14 dBm
  Tx Power Level 4                             : 11 dBm
  Tx Power Level 5                             : 8 dBm
  Tx Power Level 6                             : 5 dBm
  Tx Power Level 7                             : 2 dBm
  Tx Power Level 8                             : -1 dBm
  Tx Power Configuration                       : Automatic
  Current Tx Power Level                       : 1

Phy OFDM Parameters
  Configuration                                : Automatic
  Current Channel                              : 11
```

```
    Extension Channel                            : None
    Channel Width                                : 20 MHz
    Allowed Channel List                         : 1, 2, 3, 4, 5, 6, 7, 8, 9
                                                   10, 11
    TI Threshold                                 : 0
    Antenna Type                                 : Internal
    Internal Antenna Gain (in .5 dBi units)      : 0
    Diversity                                    : Diversity enabled

    802.11n Antennas
      Tx                                         : A, B, C
      Rx                                         : A, B, C

  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                       : 15 dB
    Coverage Exception Level                     : 25%
    Client Minimum Exception Level               : 3 clients

  Rogue Containment Information
    Containment Count                            : 0
```

show ap name core-dump

To display the memory core dump information for a lightweight access point, use the **show ap name core-dump** command.

show ap name *ap-name* **core-dump**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the memory core dump information:

```
Device# show ap name 3602a core-dump

TFTP server IP : 172.31.25.21
Memory core dump file : 3602a.dump
Memory core dump file compressed : Disabled
```

show ap name data-plane

To display the data plane status of a specific Cisco lightweight access point, use the **show ap name data-plane** command.

show ap name *ap-name* **data-plane**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the data plane status of an access point:

```
Device# show ap name AP01 data-plane

                      Min Data          Data          Max Data     Last
AP Name              Round Trip      Round Trip      Round Trip    Update
------------------  --------------  --------------  -------------- --------
AP01                   0.000s          0.000s        0.000s       00:00:00
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**ccx**| **cdp**| **profile**| **service-poicy output**| **stats**| **tsm** {**all**| *client-mac*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
ccx	Displays the Cisco Client eXtensions (CCX) radio management status information.

cdp	Displays Cisco Discovery Protocol (CDP) information.
profile	Displays configuration and statistics of 802.11 profiling.
service-policy output	Displays downstream service policy information.
stats	Displays Cisco lightweight access point statistics.
tsm	Displays 802.11 traffic stream metrics statistics.
all	Displays the list of all access points to which the client has associations.
client-mac	MAC address of the client.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the service policy that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Device# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name                AP CDP State
---------------------- --------------
AP03                   Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Device# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode             : GLOBAL
 802.11b Cisco AP Interference threshold               : 10 %
 802.11b Cisco AP noise threshold                      : -70 dBm
 802.11b Cisco AP RF utilization threshold             : 80 %
 802.11b Cisco AP throughput threshold                 : 1000000 bps
 802.11b Cisco AP clients threshold                    : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

This example show how to display statistics for a specific access point:

```
Device# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
AckFailureCount................................: 0
RxIncompleteFragment...........................: 0
MulticastRxFrameCnt............................: 0
FcsErrorCount..................................: 0
TxFrameCount...................................: 0
WepUndecryptableCount..........................: 0
TxFramesDropped................................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw).........: 0
  Video Bandwidth in use(% of config bw).........: 0
  Total BW in use for Voice(%)...................: 0
  Total BW in use for SIP Preferred call(%)......: 0

Load based Voice Call Stats
  Total channel MT free..........................: 0
  Total voice MT free............................: 0
  Na Direct......................................: 0
  Na Roam........................................: 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

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
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Device# show ap name AP01 dot11 24ghz tsm all
```

show ap name dot11 cleanair

To display CleanAir configuration information that corresponds to an access point, use the **show ap name dot11 cleanair** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} **cleanair** {**air-quality**| **device**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
cleanair	Displays CleanAir configuration information.
air-quality	Displays CleanAir air-quality (AQ) data.
device	Displays CleanAir interferers for an access point on the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CleanAir air-quality information for an access point in the 802.11b network:

```
Device# show ap name AP01 dot11 24ghz cleanair air-quality

AQ = Air Quality
DFS = Dynamic Frequency Selection
```

This example shows how to display CleanAir interferers information for an access point in the 802.11b network:

```
Device# show ap name AP01 dot11 24ghz cleanair device

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
-- --------- ----- ---- ------- --- ---- ----------
```

show ap name env

To show AP environment on a specific AP, use the **show ap name env**command.

show ap name *ap-name***env**

Syntax Description

ap-name	Name of the specific AP.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show AP environment on AP1:

```
Device# show ap name ap1 env
```

show ap name ethernet statistics

To display the Ethernet statistics of a specific Cisco lightweight access point, use the **show ap name ethernet statistics** command.

show ap name *ap-name* **ethernet statistics**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the Ethernet statistics of an access point:

```
Device# show ap name 3602a ethernet statistics

Ethernet Stats for AP 3602a

Interface Name      Status   Speed       Rx Packets    Tx Packets    Discarded Packets

-----------------------------------------------------------------------------------------
GigabitEthernet0    UP       1000 Mbps   3793          5036          0
```

show ap name eventlog

To download and display the event log of a specific Cisco lightweight access point, use the **show ap name eventlog** command.

show ap name *ap-name* **eventlog**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the event log for a specific access point:

```
Device# show ap name AP01 eventlog
```

show ap gps-location summary

To show GPS location summary of all connected Cisco APs, use the **show ap gps-location summary** command.

There is no keyword or argument.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show GPS location summary of all connected Cisco APs:

```
Device# show ap gps-location summary
```

show ap name image

To display the detailed information about the predownloaded image for specified access points, use the **show ap name image** command.

show ap name *ap-name* **image**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display images present on all access points:

```
Device# show ap name 3602a image

Total number of APs  : 1
```

```
Number of APs
        Initiated                  : 0
        Predownloading             : 0
        Completed predownloading   : 0
        Not Supported              : 1
        Failed to Predownload      : 0

AP Name      Primary Image   Backup Image    Predownload Status    Predownload Ver...  Next
 Retry Time    Retry Count
-----------------------------------------------------------------------------------------------
3602a        10.0.1.234      0.0.0.0         Not supported         None                NA
                        0
```

show ap name inventory

To display inventory information for an access point, use the **show ap name inventory** command.

show ap name *ap-name* **inventory**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display inventory information for an access point:

```
Device# show ap name 3502b inventory

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 1140AG  ,  VID: V01,  SN: SIM1140K001


NAME:     , DESCR:
PID: ,  VID: ,  SN:


NAME:     , DESCR:
PID: ,  VID: ,  SN:
NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name lan port

To display LAN information, use **show ap name lan port** command.

show ap name lan portsummary |*port-id*

Syntax Description

summary	Displays brief summary for LAN information.
port-id	Port ID of the port that the LAN information will be displayed.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7SE	This command was introduced.

This example shows how to display the brief summary for LAN information:

```
Device# show ap name ap1 lan port summary
```

show ap name link-encryption

To display the link-encryption status for a specific Cisco lightweight access point, use the **show ap name link-encryption** command.

show ap name *ap-name* **link-encryption**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the link-encryption status for a specific Cisco lightweight access point:

```
Device# show ap name AP01 link-encryption

                    Encryption  Dnstream  Upstream    Last
AP Name                  State     Count     Count  Update
------------------  ----------  --------  --------  ------
AP01                 Disabled         0         0   Never
```

show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

show ap name *ap-name* **service-policy**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Device# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name tcp-adjust-mss

To display TCP maximum segment size (MSS) for an access point, use the **show ap name tcp-adjust-mss** command.

show ap name *ap-name* **tcp-adjust-mss**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display TCP MSS for an access point:

```
Device# show ap name AP01 tcp-adjust-mss

AP Name                     TCP State        MSS Size
-------------------------------------------------------
AP01                        Disabled         6146
```

show ap name wlan

To display the Basic Service Set Identifier (BSSID) value for each WLAN defined on an access point and to display WLAN statistics, use the **show ap name wlan** command.

show ap name *ap-name* **wlan** {**dot11** {**24ghz**| **5ghz**}| **statistic**}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
dot11	Displays 802.11 parameters.
24ghz	Displays 802.11b network settings.
5ghz	Displays 802.11a network settings.
statistic	Displays WLAN statistics.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display BSSID information of an access point in an 802.11b network:

```
Device# show ap name AP01 wlan dot11 24ghz

Site Name                                        : default-group
Site Description                                 :

WLAN ID  Interface  BSSID
-------------------------------------
1        default    00:00:20:00:02:00
12       default    00:00:20:00:02:0b
```

This example shows how to display WLAN statistics for an access point:

```
Device# show ap name AP01 wlan statistic

WLAN ID  : 1
WLAN Profile Name  : maria-open

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0


WLAN ID  : 12
WLAN Profile Name  : 24

   EAP Id Request Msg Timeouts           : 0
   EAP Id Request Msg Timeouts Failures  : 0
   EAP Request Msg Timeouts              : 0
   EAP Request Msg Timeouts Failures     : 0
   EAP Key Msg Timeouts                  : 0
   EAP Key Msg Timeouts Failures         : 0
```

show ap name wlandot11 service policy

To display the QoS policies for each Basic Service Set Identifier (BSSID) for an access point use commands

show apname*ap -name***wlan dot1124ghzservice-policy**

show apname*ap -name***wlan dot115ghzservice-policy**

Syntax Description

ap- name	Name of the Cisco lightweight access point.
service-policy	Service policy information for access point.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

The following example shows how to display QoS policies for each BSSID.

```
Deviceshow ap name <ap-name> wlan dot11 24ghz service-policy
```

show ap slots

To display a slot summary of all connected Cisco lightweight access points, use the **show ap slots** command.

show ap slots

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display a slot summary of all connected Cisco lightweight access points:

```
Controller# show ap slots

AP Name    Slots  AP Model    Slot0       Slot1      Slot2     Slot3
---------- ------ ----------- ----------- ---------- --------- --------
3602a      2      3502I       802.11b/g   802.11a    Unknown   Unknown
```

show ap summary

To display the status summary of all Cisco lightweight access points attached to the device, use the **show ap summary** command.

show ap summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to display a list that contains each lightweight access point name, number of slots, manufacturer, MAC address, location, and the device port number.

This example shows how to display a summary of all connected access points:

```
Controller# show ap summary

Number of APs: 1

Global AP User Name: Cisco
Global AP Dot1x User Name: Not configured

AP Name                           AP Model  Ethernet MAC    Radio MAC       State
-------------------------------------------------------------------------------------
3602a                             3502I     003a.99eb.3fa8  d0c2.8267.8b00  Registered
```

show ap tcp-adjust-mss

To display information about the Cisco lightweight access point TCP Maximum Segment Size (MSS), use the **show ap tcp-adjust-mss** command.

show ap tcp-adjust-mss

Syntax Description

This command has no keywords and arguments.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display information about the access point TCP MSS information:

```
Controller# show ap tcp-adjust-mss

AP Name                     TCP State        MSS Size
-----------------------------------------------------
3602a                       Disabled         0
```

show ap universal summary

To show universal summary of all connected Cisco APs, use the**show ap universal summary** command. There is no keyword or argument.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

This example shows how to show universal summary of all connected Cisco APs:

```
Device# show ap universal summary
```

show ap uptime

To display the up time of all connected Cisco lightweight access points, use the **show ap uptime** command.

show ap uptime

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to the display up time of all connected access points:

```
Controller# show ap uptime

Number of APs : 1

Global AP User Name : Cisco
Global AP Dot1x User Name : Not configured

AP Name Ethernet MAC    AP Up Time                     Association Up Time

------- --------------- ------------------------------ ------------------------------
3602a   003a.99eb.3fa8  5 hours 13 minutes 40 seconds  5 hours 12 minutes 15 seconds
```

show wireless ap summary

To display the status summary of all wireless access points, use the **show wireless apsummary** command.

show wirelessap summary

Syntax Description

This command has no keywords and arguments.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
10.4	This command was introduced

This example shows how to display a summary of all wireless access points:

```
Controller# show wireless ap summary
Sub-Domain Access Point Summary

Maximum AP limit: 1010
Total AP Licence Installed: 1000
Total AP Licence Available: 1000
Total AP joined :0
```

show wireless client ap

To display the clients on a Cisco lightweight access point, use the **show wireless client ap** command.

show wireless client ap [**name** *ap-name*] **dot11** {**24ghz**| **5ghz**}

Syntax Description

name *ap-name*	(Optional) Displays the name of the Cisco lightweight access point.
dot11	Displays 802.11 parameters.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **show client ap** command might list the status of automatically disabled clients. Use the **show exclusionlist** command to view clients on the exclusion list (blacklisted).

This example shows how to display client information on a specific Cisco lightweight access point in the 2.4 GHz band:

```
Device# show wireless client ap name AP01 dot11 24ghz

MAC Address       AP Id  Status     WLAN Id Authenticated
----------------- ------ ---------- ------- -------------
xx:xx:xx:xx:xx:xx 1      Associated 1       No
```

test ap name

To enable automatic testing of the path Maximum Transmit Unit (MTU) between the access point and the device, use the **test ap name** command.

test ap name *ap-name* **pmtu** {**disable size** *size*| **enable**}

Syntax Description

ap-name	Name of the target Cisco lightweight access point.
pmtu	Tests the MTU configuration for the access point.
disable	Disables path MTU testing and manually configures the MTU value in bytes.
size *size*	Specifies the path MTU size. **Note** The range is from 576 to 1700.
enable	Enables the path MTU testing for the access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable the path MTU configuration for all access points associated to the device:

```
Controller# test ap name 3602a pmtu enable
```

test capwap ap name

To test Control and Provisioning of Wireless Access Points (CAPWAP) parameters for a specific Cisco lightweight access points, use the **test capwap ap name** command.

test capwap ap name *ap-name* {**encryption** {**enable**| **disable**}| **message** *token*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.

encryption	Tests the Datagram Transport Layer Security (DTLS) encryption.
enable	Tests if DTLS encryption is enabled.
disable	Tests if DTLS encryption is disabled.
message *token*	Specifies an RRM neighbor message to send.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to test if DTLS encryption is enabled for a specific access point:

```
Controller# test capwap ap name 3602a encryption enable
```

This example shows how to test if DTLS encryption is disabled for a specific access point:

```
Controller# test capwap ap name 3602a encryption disable
```

trapflags ap

To enable the sending of specific Cisco lightweight access point traps, use the **trapflags ap** command. To disable the sending of Cisco lightweight access point traps, use the **no** form of this command.

trapflags ap {**register**| **interfaceup**}

no trapflags ap {**register**| **interfaceup**}

Syntax Description

register	Enables sending a trap when a Cisco lightweight access point registers with a Cisco switch.
interfaceup	Enables sending a trap when a Cisco lightweight access point interface (A or B) comes up.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to prevent traps from sending access point-related traps:

```
Device(config)# no trapflags ap register
```

PART VIII

Mobility

- Mobility Commands, page 513

CHAPTER 9

Mobility Commands

- mobility anchor, page 513
- wireless mobility, page 515
- wireless mobility controller, page 515
- wireless mobility controller (ip_address) , page 517
- wireless mobility controller peer-group, page 517
- wireless mobility group keepalive, page 518
- wireless mobility group member ip, page 519
- wireless mobility group name , page 520
- wireless mobility load-balance, page 521
- show wireless mobility, page 522
- clear wireless mobility statistics, page 523

mobility anchor

To configure mobility sticky anchoring, use the **mobility anchor sticky** command. To disable the sticky anchoring, use the **no** form of the command.

To configure guest anchoring, use the **mobility anchor** *ip-address* command.

To delete the guest anchor, use the **no** form of the command.

To configure the device as an auto-anchor, use the **mobility anchor** command.

mobility anchor {*ip-address*| **sticky**}

no mobility anchor {*ip-address*| **sticky**}

Syntax Description

sticky	The client is anchored to the first switch that it associates. **Note** This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.
ip-address	Configures the IP address for the guest anchor device to this WLAN.

Command Default

Sticky configuration is enabled by default.

Command Modes

WLAN Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The auto-anchor configuration required the device IP address to be entered prior to the Cisco IOS XE 3.3SE release; with this release, if no IP address is given, the device itself becomes an anchor; you do not have to explicitly specify the IP address.

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.
- Mobility uses the following ports, that are allowed through the firewall:
  - 16666
  - 16667
  - 16668

This example shows how to enable the sticky mobility anchor:

```
Device(config-wlan)# mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Device(config-wlan)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Device(config-wlan)# mobility anchor
```

wireless mobility

To configure the inter mobility manager, use the **wireless mobility** command.

wireless mobility {**dscp** *value* }

Syntax Description

dscp *value*	Configures the Mobility inter DSCP value.

Command Default

The default DSCP value is 48.

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shoes how to configure mobility inter DSCP with an value of 20:

```
Device(config)# wireless mobility dscp 20
```

wireless mobility controller

To configure mobility controller settings, use the **wireless mobility controller** command. To remove a mobility controller settings, use the **no** form of the command.

wireless mobility controller peer-group *peer-group-name* [**bidge-domain-id** *id* | **member ip** *ip-address* [**public-ip** | *public-ip-address*]| **multicast ip** *multicast-address*]

nowireless mobility controller peer-group *peer-group-name* [**bidge-domain-id** *id* | **member ip** *ip-address* [**public-ip** | *public-ip-address*]| **multicast ip** *multicast-address*]

Syntax Description

peer-group *peer-group-name*	Creates a mobility peer group.
bidge-domain-id *id*	Configures bridge domain ID for the mobility peer group.
member ip *ip-address* **public-ip** *public-ip-address*	Adds or deletes a peer group member. **Note** The **public-ip** *public-ip-address* is optional and is only when the mobility peer is NATed.
multicast ip *multicast-address*	Configures multicast settings of a peer group.

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the Converged Access solution, WLANs are mapped to VLANs, and VLANs are usually mapped to subnets. For seamless roaming, the same VLAN configured on two controllers is expected to be mapped to the same subnet. This identical mapping from one controller to the next is important for roaming, because the controllers taking care of the roaming event need to determine if they need:

- To address a Layer 2 roaming event (when WLAN to VLAN and subnet mapping are identical on the anchor and the foreign controller), or
- a Layer 3 roaming event (when WLAN to VLAN and subnet mapping are different between the anchor and the foreign controller).

This determination is made by comparing the WLAN SSID string and the VLAN ID between controllers. In cases where the WLAN SSID and VLAN ID are identical, the expectation is that the subnet associated to the VLAN is identical as well.

There may be cases where this mapping is not identical. For example, suppose that WLAN1 on controller 1 is mapped to VLAN 14, and that VLAN 14 on controller1 is mapped to the subnet 10.10.14.0/24. Also suppose that WLAN 1 on controller2 is mapped to VLAN 14, but that VLAN 14 on controller2 is mapped to this subnet 172.31.24.0/24. Controllers 1 and 2 will compare WLAN1 and the associated VLAN and conclude that they are addressing a Layer 2 roaming event, whereas the roaming even is Layer 3, as VLAN 14 does not have the same Layer 3 significance on both controllers.

When this disconnect between VLANs and their associated subnet occurs, you may want to configure your Converged Access controllers for different bridge domain IDs. Two controllers in the same bridge domain ID are expected to have the same VLAN to subnet mapping. We recommend that you configure the same bridge domain ID on all controllers that share the same VLAN to subnet mapping, and between which roaming is expected.

This example shows how to configure a bridge domain ID.

```
Device (config)# wireless mobility controller peer-group SPG1 bridge-domain-id 111
```

This example shows how to create and configure a peer group with a bridge ID of 111:

```
Device(config)# controller peer-group TestDocPeerGroup bridge-domain-id 111
```

This example shows how to disable a peer group with a bridge ID of 111:

```
Device(config)# no controller peer-group TestDocPeerGroup bridge-domain-id 111
```

This examples shows the configuration for a NATed member (the IP 172.19.13.15 is outside the NAT):

```
Device (config)# wireless mobility group ip 1.4.91.2 public-ip 172.19.13.15
```

This examples shows the configuration of a member when it is not NATed (the IP 1.4.91.2 is inside the NAT):

```
Device (config)# wireless mobility group ip 1.4.91.2
```

wireless mobility controller (ip_address)

To configure the mobility controller, use the **wireless mobility controller** command.

To convert the switch from MC to MA, use the **no wireless mobility controller**form of the command.

To delete the mobility controllers IP address, use the **no wirelessmobility controller** ip-address

wireless mobility controller [**ip** *ip-address* [**public-ip** *public-ip-address*]]

no wireless mobility controller

no wireless mobility controllerip *ip-address*

Syntax Description

ip *ip-address*	IP address of mobility controller.
public-ip *public-ip-address*	

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is valid only for the converged access switch.

The NAted address is used to establish communication, and the configured Wireless Management interface is used to identify the peer controller during the CAPWAP exchanges.

This examples shows how the controller communicates with the wireless management interface :

```
Device (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6
```

This examples shows how to add a NAT option along with the wireless managed interface, when the target controller uses NAT:

```
Device (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip
 10.21.21.2
```

wireless mobility controller peer-group

To configure mobility peer groups, use the **wireless mobility controller peer-group** command, to remove the configuration, use the **no** form of this command.

wireless mobility controller peer-group *peer-group* **member IP** *ip-address***mode centralized**

Syntax Description

peer group	Name of the peer group.
member IP	Adds a peer group member.
ip-address	IP address of the peer group member to be added.
mode centralized	Configures the management mode of the peer group member as centrally managed.

Command Default

The centralized mode is off.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

```
Device enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless mobility controller peer-group peer1 member ip 10.0.0.1 mode
centralized
```

wireless mobility group keepalive

To configure the mobility group parameter and keep alive its ping parameters, use the **wireless mobility group keepalive** command. To remove a mobility group parameter, use the **no** form of the command.

wireless mobility group keepalive {**count** *number*| **interval** *interval*}

no wireless mobility group keepalive {**count** *numbe r*| **interval** *interval*}

Syntax Description

count *number*	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.
interval *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

3 seconds for count and 10 seconds for interval.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The default values for *interval* is ten seconds and the default for *retries* is set to three.

This example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:

```
Device(config)# wireless mobility group keepalive count 10
```

wireless mobility group member ip

To add or delete users from mobility group member list, use the **wireless mobility group member ip** command. To remove a member from the mobility group, use the **no** form of the command.

wireless mobility group member ip *ip-address* [**public-ip** *public-ip-address*] [**group** *group-name*]

no wireless mobility group member ip *ip-address*

Syntax Description

ip-address	The IP address of the member controller.
public-ip *public-ip-address*	(Optional) Member controller public IP address. **Note** This command is used only when the member is behind a NAT. Only static IP NAT is supported.
group *group-name*	(Optional) Member controller group name. **Note** This command is used only when the member added in not in the same group as the local mobility controller.

Command Default

None.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The mobility group is used when there is more than one Mobility Controller (MC) in a given deployment. The mobility group can be assigned with a name or it can use the default group name. The mobility group members need to be configured on all the members of the group to roam within the group.

This example shows how to add a member in a mobility group:

```
Device(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group name

To configure hte mobility domain name, use the **wireless mobility group name** command. To remove the mobility domain name, use the **no** form of the command.

Note If you are configuring the mobility group in a network where network address translation (NAT) is enabled, enter the IP address that is sent to the controller from the NAT device rather than the controller's management interface IP address. Otherwise, mobility will fail among controllers in the mobility group.

wireless mobility group name *domain-name*

no wireless mobility group name

Syntax Description

domain-name	Creates a mobility group by entering this command. The domain name can be up to 31 case-sensitive characters.

Command Default

Default.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a mobility domain name lab1:

```
Device(config)# mobility group domain lab1
```

wireless mobility load-balance

This command is used to load-balance the mobile clients on a mobility anchor (MA) from a switch peer group (SPG) that is least loaded and is chosen to act as the point of presence for the mobile client.

To configure the mobility load-balance status, use the **wireless mobility load-balance** command.

To disable the mobility load-balance, use the **no wirelessmobility load-balance**form of the command.

To configure the client load on the switch where mobility load-balance is turned on, use the **no wirelessmobility load-balance** threshold form of the command.

wireless mobility load-balance [**threshold** *threshold*]

[**no**]**wireless mobility load-balance [threshold]**

[**no**]**wireless mobility load-balance**

Syntax Description

threshold *threshold*	Configures the threshold for the number of clients that can be anchored locally.

Command Default

Load balance enabled and set at a value of 1000.

Command Modes

Global Configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

- This command is only supported on a mobility agent.
- By default, the threshold can accommodate more than fifty percent of the total clients on the node. Any client joining the switch after the reaching the configured threshold value is automatically anchored to the least loaded switch within the same switch peer group.

This example shows how to configure the mobility load-balance status with a threshold set at 150.

```
Device(config)# wireless mobility load-balance threshold 150
```

show wireless mobility

To view the wireless mobility summary, use the **show wireless mobility** command.

show wireless mobility {**load-balance summary agent** *mobility-agent-ip* **client summary** |**ap-list ip-address** *ip-address*| **controller client summary**|**dtls connections**|**statistics summary**}

Syntax Description

load-balance summary	Shows the mobility load-balance properties.
agent *mobility-agent-ip* **client summary**	Shows the active clients on a mobility agent.
ap-list ip-address *ip-address*	Shows the list of Cisco APs known to the mobility group.
controller client summary	Shows the active clients in the subdomain.
dtls connections	Shows the DTLS server status.
statistics	Shows the statistics for the Mobility manager.
summary	Shows the summary of the mobility manager.

Command Default

None

Command Modes

Global Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display a summary of the mobility manager:

```
Device (config)# show wireless mobility ap-list

AP name                          AP radio MAC      Controller IP     Learnt from
-------------------------------------------------------------------------------------------
TSIM_AP-101                      0000.2000.6600    9.9.9.2           Self
TSIM_AP-102                      0000.2000.6700    9.9.9.2           Self
TSIM_AP-103                      0000.2000.6800    9.9.9.2           Self
TSIM_AP-400                      0000.2001.9100    9.9.9.2           Self
TSIM_AP-402                      0000.2001.9300    9.9.9.2           Self
TSIM_AP-403                      0000.2001.9400    9.9.9.2           Self
TSIM_AP-406                      0000.2001.9700    9.9.9.2           Self
TSIM_AP-407                      0000.2001.9800    9.9.9.2           Self
TSIM_AP-409                      0000.2001.9a00    9.9.9.2           Self
```

clear wireless mobility statistics

To clear wireless statistics, use the **clear wireless mobility statistics** command.

clear wireless mobility statistics

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can clear all the information by using the **clear wireless mobility statistics** command.

This example shows how to clear wireless mobility statistics:

```
Device (config)# clear wireless mobility statistics
```

PART IX

Network Management

- Network Management Commands, page 527

CHAPTER 10

Network Management Commands

- ip wccp, page 528
- monitor capture (interface/control plane), page 530
- monitor capture buffer, page 534
- monitor capture clear, page 535
- monitor capture export, page 535
- monitor capture file, page 536
- monitor capture limit, page 538
- monitor capture match, page 539
- monitor capture start, page 540
- monitor capture stop, page 540
- monitor session, page 541
- monitor session destination, page 542
- monitor session filter, page 546
- monitor session source, page 547
- show ip sla statistics, page 549
- show monitor, page 550
- show monitor capture, page 552
- show platform ip wccp, page 553
- show platform software swspan , page 554
- snmp-server enable traps, page 556
- snmp-server enable traps bridge, page 558
- snmp-server enable traps bulkstat, page 559
- snmp-server enable traps call-home, page 560
- snmp-server enable traps cef, page 561

- snmp-server enable traps cpu, page 562
- snmp-server enable traps envmon, page 563
- snmp-server enable traps errdisable, page 564
- snmp-server enable traps flash, page 565
- snmp-server enable traps isis, page 566
- snmp-server enable traps license, page 566
- snmp-server enable traps mac-notification, page 567
- snmp-server enable traps ospf, page 568
- snmp-server enable traps pim, page 569
- snmp-server enable traps port-security, page 570
- snmp-server enable traps power-ethernet, page 571
- snmp-server enable traps snmp, page 572
- snmp-server enable traps stackwise, page 573
- snmp-server enable traps storm-control, page 575
- snmp-server enable traps stpx, page 576
- snmp-server enable traps transceiver, page 577
- snmp-server enable traps vrfmib, page 578
- snmp-server enable traps vstack, page 579
- snmp-server engineID, page 580
- snmp-server host, page 580
- switchport mode access, page 585
- switchport voice vlan, page 586

ip wccp

To enable the web cache service, and specify the service number that corresponds to a dynamic service that is defined by the application engine, use the **ip wccp** global configuration command on the device. Use the **no** form of this command to disable the service.

ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

no ip wccp {**web-cache** | *service-number*} [**group-address** *groupaddress*] [**group-list** *access-list*] [**redirect-list** *access-list*] [**password** *encryption-number password*]

Syntax Description

web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2).

service-number	Dynamic service identifier, which means the service definition is dictated by the cache. The dynamic service number can be from 0 to 254. The maximum number of services is 256, which includes the web-cache service specified with the **web-cache** keyword.
group-address *groupaddress*	(Optional) Specifies the multicast group address used by the devices and the application engines to participate in the service group.
group-list *access-list*	(Optional) If a multicast group address is not used, specifies a list of valid IP addresses that correspond to the application engines that are participating in the service group.
redirect-list *access-list*	(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.
password *encryption-number password*	(Optional) Specifies an encryption number. The range is 0 to 7. Use 0 for not encrypted, and use 7 for proprietary. Also, specifies a password name up to seven characters in length. The device combines the password with the MD5 authentication value to create security for the connection between the device and the application engine. By default, no password is configured, and no authentication is performed.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a device to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once.

Example

The following example configures a web cache, the interface connected to the application engine or the server, and the interface connected to the client:

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec  6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

monitor capture (interface/control plane)

To configure monitor capture points specifying an attachment point and the packet flow direction or add more attachment points to a capture point, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction or disable one of multiple attachment points on a capture point, use the **no** form of this command.

monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

no monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

Syntax Description

capture-name	The name of the capture to be defined.

interface *interface-type interface-id*	Specifies an interface with *interface-type* and *interface-id* as an attachment point. The arguments have these meanings: • **GigabitEthernet** *interface-id*—A Gigabit Ethernet IEEE 802.3z interface. • **vlan** *vlan-id*—A VLAN. The range for *vlan-id* is 1 to 4095. • **capwap** *capwap-id*—Specifies a Control and Provisioning of Wireless Access Points Protocol (CAPWAP) tunneling interface. For a list of CAPWAP tunnels that can be used as attachment points, use the **show capwap summary** command. **Note** This is the only attachment point that can be used for a wireless capture. When using this interface as an attachment point, no other interface types can be used as attachment points on the same capture point.
control-plane	Specifies the control plane as an attachment point.
in | **out** | **both**	Specifies the traffic direction to be captured.

Command Default

A Wireshark capture is not configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Once an attachment point has been associated with a capture point using this command, the only way to change its direction is to remove the attachment point using the **no** form of the command and reattach the attachment point with the new direction. An attachment point's direction cannot be overridden.

If an attachment point is removed from a capture point and only one attachment point is associated with it, the capture point is effectively deleted.

Multiple attachment points can be associated with a capture point by re-running this command with another attachment point. An example is provided below.

Multiple capture points can be defined, but only one can be active at a time. In other words, you have to stop one before you can start the other.

Packets captured in the output direction of an interface might not reflect the changes made by switch rewrite (includes TTL, VLAN tag, CoS, checksum, MAC addresses, DSCP, precedent, UP, etc.).

No specific order applies when defining a capture point; you can define capture point parameters in any order. The Wireshark CLI allows as many parameters as possible on a single line. This limits the number of commands required to define a capture point.

Neither VRFs, management ports, nor private VLANs can be used as attachment points.

Wireshark cannot capture packets on a destination SPAN port.

When a VLAN is used as a Wireshark attachment point, packets are captured in the input direction only.

Wireless (CAPWAP) Usage Considerations

The only form of wireless capture is a CAPWAP tunnel capture.

When capturing CAPWAP tunnels, no other interface types can be used as attachment points on the same capture point.. Also, the only different type of attachment point allowed on the same capture point is the control plane. The combination of control plane and CAPWAP tunnel attachment points should be able to capture all wireless-related traffic.

Capturing multiple CAPWAP tunnels is supported. ACLs for each CAPWAP tunnel will be combined and sent to the switch as a single ACL.

Core filters will not be applied and can be omitted when capturing a CAPWAP tunnel. When control plane and CAPWAP tunnels are mixed, the core filter will not be applied on the control plane packets either.

To capture a CAPWAP non-data tunnel, capture traffic on the management VLAN and apply an appropriate ACL to filter the traffic. Note that this ACL will be combined with the core filter ACL and assigned to the switch as a single ACL.

Examples

To define a capture point using a physical interface as an attachment point:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

Note The second command defines the core filter for the capture point. This is required for a functioning capture point unless you are using a CAPWAP tunneling attachment point in your capture point.

If you are using CAPWAP tunneling attachment points in your capture point, you cannot use core filters.

To define a capture point with multiple attachment points:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
```

To remove an attachment point from a capture point defined with multiple attachment points:

```
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
   monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
   monitor capture mycap interface GigabitEthernet1/0/1 in
```

To define a capture point with a CAPWAP attachment point:

```
Device# show capwap summary

CAPWAP Tunnels General Statistics:
  Number of Capwap Data Tunnels       = 1
  Number of Capwap Mobility Tunnels   = 0
  Number of Capwap Multicast Tunnels  = 0
```

```
Name   APName                           Type PhyPortIf Mode      McastIf
------ ------------------------------- ---- --------- --------- -------
Ca0    AP442b.03a9.6715                data Gi3/0/6   unicast   -

Name   SrcIP           SrcPort DestIP          DstPort DtlsEn MTU   Xact
------ --------------- ------- --------------- ------- ------ ----- ----
Ca0    10.10.14.32     5247    10.10.14.2      38514   No     1449  0

Device# monitor capture mycap interface capwap 0 both
Device# monitor capture mycap file location flash:mycap.pcap
Device# monitor capture mycap file buffer-size 1
Device# monitor capture mycap start

*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on

Device# show monitor capture mycap parameter
   monitor capture mycap interface capwap  0 in
   monitor capture mycap interface capwap  0 out
   monitor capture mycap file location flash:mycap.pcap buffer-size 1
Device#
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
Device#
Device# show monitor capture file flash:mycap.pcap
  1   0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  2   0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  3   2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  4   2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  5   3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  6   4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  7   4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  8   5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
  9   5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 10   6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 11   8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
 Flags=........
 12   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 13   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 14   9.225986   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
 15   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
```

```
16   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
17   9.231998   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
18   9.236987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
19  10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
20  10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
21  12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
22  12.239993   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
23  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
24  12.244997   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
25  12.250994   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
26  12.256990   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
27  12.262987   10.10.14.2 -> 10.10.14.32  DTLSv1.0 Application Data
28  12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
29  12.802012   10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30  13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=........
```

monitor capture buffer

To configure the buffer for monitor capture (WireShark), use the **monitor capture buffer** command in privileged EXEC mode. To disable the monitor capture buffer or change the buffer back to a default linear buffer from a circular buffer, use the **no** form of this command.

monitor capture {*capture-name*} **buffer** {**circular** [**size** *buffer-size*] | **size** *buffer-size*}

no monitor capture {*capture-name*} **buffer** [**circular**]

Syntax Description

capture-name	The name of the capture whose buffer is to be configured.
circular	Specifies that the buffer is of a circular type. The circular type of buffer continues to capture data, even after the buffer is consumed, by overwriting the data captured previously.
size *buffer-size*	(Optional) Specifies the size of the buffer. The range is from 1 MB to 100 MB.

Command Default

A linear buffer is configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

When you first configure a WireShark capture, a circular buffer of a small size is suggested.

Example

To configure a circular buffer with a size of 1 MB:

```
Device# monitor capture mycap buffer circular size 1
```

monitor capture clear

To clears the monitor capture (WireShark) buffer, use the **monitor capture clear** command in privileged EXEC mode.

monitor capture {*capture-name*} **clear**

Syntax Description

capture-name	The name of the capture whose buffer is to be cleared.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command either during capture or after the capture has stopped either because one or more end conditions has been met, or you entered the **monitor capture stop** command. If you enter the **monitor capture clear** command after the capture has stopped, the **monitor capture export** command that is used to store the contents of the captured packets in a file will have no impact because the buffer has no captured packets.

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Example

To clear the buffer contents for capture mycap:

```
Device#  monitor capture mycap clear
```

monitor capture export

To export a monitor capture (WireShark) to a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture {*capture-name*} **export** *file-location* : *file-name*

Syntax Description

capture-name	The name of the capture to be exported.
file-location : *file-name*	(Optional) Specifies the location and file name of the capture storage file. Acceptable values for *file-location* : • flash—On-board flash storage • (usbflash0:)— USB drive

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When WireShark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.

Note Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To export the capture buffer contents to mycap.pcap on a flash drive:

```
Device# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

To configure monitor capture (WireShark) storage file attributes, use the **monitor capture file** command in privileged EXEC mode. To remove a storage file attribute, use the **no** form of this command.

monitor capture {*capture-name*} **file**{[**buffer-size** *temp-buffer-size*][**location** *file-location* : *file-name*][**ring** *number-of-ring-files*][**size** *total-size*]}

no monitor capture {*capture-name*} **file**{[**buffer-size**][**location**][**ring**][**size**]}

Syntax Description

capture-name	The name of the capture to be modified.
buffer-size *temp-buffer-size*	(Optional) Specifies the size of the temporary buffer. The range for *temp-buffer-size* is 1 to 100 MB. This is specified to reduce packet loss.
location *file-location* : *file-name*	(Optional) Specifies the location and file name of the capture storage file. Acceptable values for *file-location* : • flash—On-board flash storage • (usbflash0:)— USB drive
ring *number-of-ring-files*	(Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring.
size *total-size*	(Optional) Specifies the total size of the capture files.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture file** command only when the storage destination is a file. The file may be stored either remotely or locally. Use this command after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When WireShark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.

Note Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To specify that the storage file name is mycap.pcap, stored on a flash drive:

```
Device# monitor capture mycap file location flash:mycap.pcap
```

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

monitor capture {*capture-name*} **limit** {[**duration** *seconds*][**packet-length** *size*][**packets** *num*]}

no monitor capture {*capture-name*} **limit** [**duration**][**packet-length**][**packets**]

Syntax Description

capture-name	The name of the capture to be assigned capture limits.
duration *seconds*	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
packet-length *size*	(Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the bytes argument is stored.
packets *num*	(Optional) Specifies the number of packets to be processed for capture.

Command Default

Capture limits are not configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

To configure a session limit of 60 seconds and a packet segment length of 400 bytes:

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match

Note Do not use this command when capturing a CAPWAP tunnel. Also, when control plane and CAPWAP tunnels are mixed, this command will have no effect.

To define an explicit inline core filter for a monitor (Wireshark) capture, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture {*capture-name*} **match** {**any** | **mac** *mac-match-string* | **ipv4** {**any** | **host** | **protocol**}{**any** | **host**} | **ipv6** {**any** | **host** | **protocol**}{**any** | **host**}}

no monitor capture {*capture-name*} **match**

Syntax Description

capture-name	The name of the capture to be assigned a core filter.
any	Specifies all packets.
mac *mac-match-string*	Specifies a Layer 2 packet.
ipv4	Specifies IPv4 packets.
host	Specifies the host.
protocol	Specifies the protocol.
ipv6	Specifies IPv6 packets.

Command Default

A core filter is not configured.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Examples

To define a capture point and the core filter for the capture point that matches to any IP version 4 packets on the source or destination:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture {*capture-name*} **start**

Syntax Description

capture-name	The name of the capture to be started.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Example

To start capturing buffer contents:

```
Device#  monitor capture mycap start
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture {*capture-name*} **stop**

Syntax Description

capture-name	The name of the capture to be stopped.

Command Default

The packet data capture is ongoing.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **monitor capture stop** command to stop the capture of packet data that you started using the **monitor capture start** command. You can configure two types of capture buffers: linear and circular. When the linear buffer is full, data capture stops automatically. When the circular buffer is full, data capture starts from the beginning and the data is overwritten.

Example

To stop capturing buffer contents:

```
Device#  monitor capture mycap stop
```

monitor session

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

monitor session *session-number* {**destination** | **filter** | **source**}

no monitor session {*session-number* [**destination** | **filter** | **source**] | **all** | **local** | **range** *session-range* | **remote**}

Syntax Description

session-number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
all	Clears all monitor sessions.
local	Clears all local monitor sessions.
range *session-range*	Clears monitor sessions in the specified range.
remote	Clears all remote monitor sessions.

Command Default

No monitor sessions are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Example

This example shows how to create a local SPAN session 1 to monitor traffic on Po13 (an EtherChannel port) and limit SPAN traffic in the session only to VLAN 1281. Egress traffic replicates the source; ingress forwarding is not enabled.

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
 replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
 replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Device# show monitor session all

Session 1
---------
Type                    : Local Session
Source Ports            :
    Both                : Po13
Destination Ports      : Gi2/0/36,Gi3/0/36
    Encapsulation      : Replicate
          Ingress      : Disabled
Filter VLANs           : 1281
...
```

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

no monitor session *session-number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation** {**replicate** | **dot1q**}] {**ingress** [**dot1q** | **untagged**] } | {**remote**} **vlan** *vlan-id*

Syntax Description

session-number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
interface *interface-id*	Specifies the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 128.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
encapsulation replicate	(Optional) Specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged). These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The **encapsulation** options are ignored with the **no** form of the command.
encapsulation dot1q	(Optional) Specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation. These keywords are valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore, packets are always sent untagged. The **encapsulation** options are ignored with the **no** form of the command.
ingress	Enables ingress traffic forwarding.
dot1q	(Optional) Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.
untagged	(Optional) Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.
isl	Specifies ingress forwarding using ISL encapsulation.

remote	Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
vlan *vlan-id*	Sets the default VLAN for ingress traffic when used with only the **ingress** keyword.

Command Default

No monitor sessions are configured.

If **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

You can specify **all**, **local**, **range** *session-range*, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of 8 local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

A SPAN or RSPAN destination must be a physical port.

You can have a maximum of 64 destination ports on a switch or a switch stack.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

EtherChannel ports can be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x authentication is disabled until the port is removed as a SPAN destination. If IEEE 802.1x authentication is not available on the port, the switch returns an error message. You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to function in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow**—dot1q** or **untagged**.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow**—dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Device(config)# monitor session 10 source remote vlan 900
```

```
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
 dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
 vlan 5
```

monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

no monitor session *session-number* **filter** {**vlan** *vlan-id* [**,** | **-**] }

Syntax Description

session-number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
vlan *vlan-id*	Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The *vlan-id* range is 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.

Command Default

No monitor sessions are configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (**-**).

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2 and to filter IPv4 traffic using access list number 122 in an FSPAN session:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 1 filter ip access-group 122
```

monitor session source

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source session, or to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session source** global configuration command. To remove the SPAN or RSPAN session or to remove source interfaces from the SPAN or RSPAN session, use the **no** form of this command.

monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

no monitor session *session_number* **source** {**interface** *interface-id* [**,** | **-**] [**both** | **rx** | **tx**] | [**remote**] **vlan** *vlan-id* [**,** | **-**] [**both** | **rx** | **tx**]}

Syntax Description

session_number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.

interface *interface-id*	Specifies the source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type, stack member, module, and port number). For source interface, port channel is also a valid interface type, and the valid range is 1 to 48.
,	(Optional) Specifies a series of interfaces or VLANs, or separates a range of interfaces or VLANs from a previous range. Enter a space before and after the comma.
-	(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.
both | **rx** | **tx**	(Optional) Specifies the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic.
remote	(Optional) Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).
vlan *vlan-id*	When used with only the **ingress** keyword, sets default VLAN for ingress traffic.

Command Default

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

A source can be a physical port, a port channel, or a VLAN.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x authentication on a SPAN or RSPAN source port.

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN, RSPAN, FSPAN, and FRSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 on stack member 1 to destination port 2 on stack member 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

show ip sla statistics

To display current or aggregated operational status and statistics of all Cisco IOS IP Service Level Agreement (SLA) operations or a specified operation, use the **show ip sla statistics** command in user EXEC or privileged EXEC mode.

show ip sla statistics [*operation-number* [**details**] | **aggregated** [*operation-number* | **details**] | **details**]

Syntax Description

operation-number	(Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
details	(Optional) Specifies detailed output.
aggregated	(Optional) Specifies the IP SLA aggregated statistics.

Command Default

Displays output for all running IP SLA operations.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip sla statistics** to display the current state of IP SLA operations, including how much life the operation has left, whether the operation is active, and the completion time. The output also includes the monitoring data returned for the last (most recently completed) operation. This generated operation ID is displayed when you use the **show ip sla** configuration command for the base multicast operation, and as part of the summary statistics for the entire operation.

Enter the **show** command for a specific operation ID to display details for that one responder.

Examples

The following is sample output from the **show ip sla statistics** command:

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200  OK
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
```

show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor** command in EXEC mode.

show monitor [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]]

Syntax Description

session	(Optional) Displays information about specified SPAN sessions.
session_number	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
all	(Optional) Displays all SPAN sessions.
local	(Optional) Displays only local SPAN sessions.
range *list*	(Optional) Displays a range of SPAN sessions, where *list* is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges. **Note** This keyword is available only in privileged EXEC mode.
remote	(Optional) Displays only remote SPAN sessions.
detail	(Optional) Displays detailed information about the specified sessions.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The output is the same for the **show monitor** command and the **show monitor session all** command.

Maximum number of SPAN source sessions: 2 (applies to source and local sessions)

Examples

This is an example of output for the **show monitor** user EXEC command:

```
Device# show monitor
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
```

```
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
---------
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105
```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```
Device# show monitor session 1
Session 1
---------
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Device# show monitor session all
Session 1
---------
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
---------
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/012
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

show monitor capture

To display monitor capture (WireShark) content, use the **show monitor capture file** command in privileged EXEC mode.

show monitor capture [*capture-name* [**buffer**] | **file** *file-location* : *file-name*][**brief** | **detailed** | **display-filter** *display-filter-string*]

Syntax Description

capture-name	(Optional) Specifies the name of the capture to be displayed.
buffer	(Optional) Specifies that a buffer associated with the named capture is to be displayed.

file *file-location* : *file-name*	(Optional) Specifies the file location and name of the capture storage file to be displayed.
brief	(Optional) Specifies the display content in brief.
detailed	(Optional) Specifies detailed display content.
display-filter *display-filter-string*	Filters the display content according to the *display-filter-string*.

Command Default

Displays all capture content.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

none

Example

To display the capture for a capture called mycap:

```
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
    Ingress:
 0
    Egress:
 0
   Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
   Buffer Type: LINEAR (default)
  File Details:
   Associated file name: flash:mycap.pcap
   Size of buffer(in MB): 1
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Packets per second: 0 (no limit)
   Packet sampling rate: 0 (no sampling)
```

show platform ip wccp

To display platform-dependent Web Cache Communication Protocol (WCCP) information, use the **show platform ip wccp** privileged EXEC command.

show platform ip wccp {**cache-engines | interfaces | service-groups**} [**switch** *switch-number*]

Syntax Description

cache-engines	Displays WCCP cache engines.
interfaces	Displays WCCP interfaces.
service-groups	Displays WCCP service groups.
switch *switch-number*	(Optional) Displays WCCP information only for specified *switch-number*.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is available only if your device is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Device# show platform ip wccp interfaces

WCCP Interfaces


**** WCCP Interface Gi1/0/3 iif_id:0x104a60000000087 (#SG:1), vrf:0 Ingress
le_handle:0x565dd208 IPv4 Sw-Label:3, Asic-Label:3

* Service group id:0 type: Well-known    token:126 vrf:0 (ref count:1)
Open service    prot: PROT_TCP  l4_type: Dest ports     priority: 240
port[0]: 80
```

show platform software swspan

To display switched port analyzer (SPAN) information, use the **show platform software swspan** command in privileged EXEC mode.

show platform software swspan {**switch**} {{{**F0 | FP active**} **counters**}| **R0 | RP active**} {**destination sess-id** *session-ID* | **source sess-id** *session-ID*}

Syntax Description

switch	Displays information about the switch.

F0	Displays information about the Embedded Service Processor (ESP) slot 0.
FP	Displays information about the ESP.
active	Displays information about the active instance of the ESP or the Route Processor (RP).
counters	Displays the SWSPAN message counters.
R0	Displays information about the RP slot 0.
RP	Displays information the RP.
destination sess-id *session-ID*	Displays information about the specified destination session.
source sess-id *session-ID*	Displays information about the specified source session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced in a release prior to Cisco IOS XE Denali 16.1.1.

Usage Guidelines

If the session number does not exist or if the SPAN session is a remote destination session, the command output will display the following message "% Error: No Information Available."

The following is sample output from the **show platform software swspan FP active source** command:

```
Switch# show platform software swspan FP active source sess-id 0

Showing SPAN source detail info

Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
Parent AOM object Status : Done

Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
```

```
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

The following is sample output from the **show platform software swspan RP active destination** command:

```
Switch# show platform software swspan RP active destination

Showing SPAN destination table summary info

Sess-id IF-type IF-id Sess-type
--------------------------------------
1 PORT 19 Remote
```

snmp-server enable traps

To enable the device to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

no snmp-server enable traps [**auth-framework** [**sec-violation**] | **bridge** | **call-home** | **cluster** | **config** | **config-copy** | **config-ctid** | **copy-config** | **cpu** | **dot1x** | **energywise** | **entity** | **envmon** | **errdisable** | **event-manager** | **flash** | **fru-ctrl** | **license** | **mac-notification** | **port-security** | **power-ethernet** | **rep** | **snmp** | **stackwise** | **storm-control** | **stpx** | **syslog** | **transceiver** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete** | **vstack** | **vtp**]

Syntax Description

auth-framework	(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
sec-violation	(Optional) Enables SNMP camSecurityViolationNotif notifications.
bridge	(Optional) Enables SNMP STP Bridge MIB traps.*
call-home	(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
cluster	(Optional) Enables SNMP cluster traps.
config	(Optional) Enables SNMP configuration traps.
config-copy	(Optional) Enables SNMP configuration copy traps.
config-ctid	(Optional) Enables SNMP configuration CTID traps.
copy-config	(Optional) Enables SNMP copy-configuration traps.

cpu	(Optional) Enables CPU notification traps.*
dot1x	(Optional) Enables SNMP dot1x traps.*
energywise	(Optional) Enables SNMP energywise traps.*
entity	(Optional) Enables SNMP entity traps.
envmon	(Optional) Enables SNMP environmental monitor traps.*
errdisable	(Optional) Enables SNMP errdisable notification traps.*
event-manager	(Optional) Enables SNMP Embedded Event Manager traps.
flash	(Optional) Enables SNMP FLASH notification traps.*
fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack.
license	(Optional) Enables license traps.*
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
port-security	(Optional) Enables SNMP port security traps.*
power-ethernet	(Optional) Enables SNMP power Ethernet traps.*
rep	(Optional) Enables SNMP Resilient Ethernet Protocol traps.
snmp	(Optional) Enables SNMP traps.*
stackwise	(Optional) Enables SNMP stackwise traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
transceiver	(Optional) Enables SNMP transceiver traps.*
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vstack	(Optional) Enables SNMP Smart Install traps.*

vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

Note Though visible in the command-line help strings, the **fru-ctrl, insertion**, and **removal** keywords are not supported on the device. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable more than one type of SNMP trap:

```
Device(config)# snmp-server enable traps cluster
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```

snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bridge [**newroot**] [**topologychange**]

no snmp-server enable traps bridge [**newroot**] [**topologychange**]

Syntax Description

newroot	(Optional) Enables SNMP STP bridge MIB new root traps.
topologychange	(Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to send bridge new root traps to the NMS:

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

To enable data-collection-MIB traps, use the **snmp-server enable traps bulkstat** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps bulkstat [**collection** | **transfer**]

no snmp-server enable traps bulkstat [**collection** | **transfer**]

Syntax Description

collection	(Optional) Enables data-collection-MIB collection traps.
transfer	(Optional) Enables data-collection-MIB transfer traps.

Command Default

The sending of data-collection-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate data-collection-MIB collection traps:

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

no snmp-server enable traps call-home [**message-send-fail** | **server-fail**]

Syntax Description

message-send-fail	(Optional) Enables SNMP message-send-fail traps.
server-fail	(Optional) Enables SNMP server-fail traps.

Command Default

The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP message-send-fail traps:

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

no snmp-server enable traps cef [**inconsistency** | **peer-fib-state-change** | **peer-state-change** | **resource-failure**]

Syntax Description

inconsistency	(Optional) Enables SNMP CEF Inconsistency traps.
peer-fib-state-change	(Optional) Enables SNMP CEF Peer FIB State change traps.
peer-state-change	(Optional) Enables SNMP CEF Peer state change traps.
resource-failure	(Optional) Enables SNMP CEF Resource Failure traps.

Command Default

The sending of SNMP CEF traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP CEF inconsistency traps:

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps cpu [**threshold**]

no snmp-server enable traps cpu [**threshold**]

Syntax Description

threshold	(Optional) Enables CPU threshold notification.

Command Default

The sending of CPU notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate CPU threshold notifications:

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps envmon [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

no snmp-server enable traps envmon [**fan**][**shutdown**][**status**] [**supply**][**temperature**]

Syntax Description

fan	(Optional) Enables fan traps.
shutdown	(Optional) Enables environmental monitor shutdown traps.
status	(Optional) Enables SNMP environmental status-change traps.
supply	(Optional) Enables environmental monitor power-supply traps.
temperature	(Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate fan traps:

```
Device(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description

notification-rate *number-of-notifications*	(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.

Command Default

The sending of SNMP notifications of error-disabling is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to set the number SNMP notifications of error-disabling to 2:

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps flash [**insertion**][**removal**]

no snmp-server enable traps flash [**insertion**][**removal**]

Syntax Description

insertion	(Optional) Enables SNMP flash insertion notifications.
removal	(Optional) Enables SNMP flash removal notifications.

Command Default

The sending of SNMP flash notifications is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP flash insertion notifications:

```
Device(config)# snmp-server enable traps flash insertion
```

snmp-server enable traps isis

To enable intermediate system-to-intermediate system (IS-IS) link-state routing protocol traps, use the **snmp-server enable traps isis** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps isis [**errors** | **state-change**]

no snmp-server enable traps isis [**errors** | **state-change**]

Syntax Description

errors	(Optional) Enables IS-IS error traps.
state-change	(Optional) Enables IS-IS state change traps.

Command Default

The sending of IS-IS traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate IS-IS error traps:

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps license [**deploy**][**error**][**usage**]

no snmp-server enable traps license [**deploy**][**error**][**usage**]

Syntax Description

deploy	(Optional) Enables license deployment traps.
error	(Optional) Enables license error traps.
usage	(Optional) Enables license usage traps.

Command Default

The sending of license traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate license deployment traps:

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps mac-notification [**change**][**move**][**threshold**]

no snmp-server enable traps mac-notification [**change**][**move**][**threshold**]

Syntax Description

change	(Optional) Enables SNMP MAC change traps.

move	(Optional) Enables SNMP MAC move traps.
threshold	(Optional) Enables SNMP MAC threshold traps.

Command Default

The sending of SNMP MAC notification traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP MAC notification change traps:

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

To enable SNMP Open Shortest Path First (OSPF) traps, use the **snmp-server enable traps ospf** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

no snmp-server enable traps ospf [**cisco-specific** | **errors** | **lsa** | **rate-limit** *rate-limit-time max-number-of-traps* | **retransmit** | **state-change**]

Syntax Description

cisco-specific	(Optional) Enables Cisco-specific traps.
errors	(Optional) Enables error traps.
lsa	(Optional) Enables link-state advertisement (LSA) traps.

rate-limit	(Optional) Enables rate-limit traps.
rate-limit-time	(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.
max-number-of-traps	(Optional) Specifies maximum number of rate-limit traps to be sent in window time.
retransmit	(Optional) Enables packet-retransmit traps.
state-change	(Optional) Enables state-change traps.

Command Default

The sending of OSPF SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable LSA traps:

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps pim [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

no snmp-server enable traps pim [**invalid-pim-message**][**neighbor-change**][**rp-mapping-change**]

Syntax Description

invalid-pim-message	(Optional) Enables invalid PIM message traps.
neighbor-change	(Optional) Enables PIM neighbor-change traps.
rp-mapping-change	(Optional) Enables rendezvous point (RP)-mapping change traps.

Command Default

The sending of PIM SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable invalid PIM message traps:

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps port-security [**trap-rate** *value*]

no snmp-server enable traps port-security [**trap-rate** *value*]

Syntax Description

trap-rate *value*	(Optional) Sets the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every occurrence).

Command Default The sending of port security SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable port-security traps at a rate of 200 per second:

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps power-ethernet {**group** *number* | **police**}

no snmp-server enable traps power-ethernet {**group** *number* | **police**}

Syntax Description

group *number*	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.
police	Enables inline power policing traps.

Command Default The sending of power-over-Ethernet SNMP traps is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable power-over-Ethernet traps for group 1:

```
Device(config)# snmp-server enable traps poower-over-ethernet group 1
```

snmp-server enable traps snmp

To enable SNMP traps, use the **snmp-server enable traps snmp** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps snmp [**authentication**][**coldstart**][**linkdown**] [**linkup**][**warmstart**]

no snmp-server enable traps snmp [**authentication**][**coldstart**][**linkdown**] [**linkup**][**warmstart**]

Syntax Description

authentication	(Optional) Enables authentication traps.
coldstart	(Optional) Enables cold start traps.
linkdown	(Optional) Enables linkdown traps.
linkup	(Optional) Enables linkup traps.
warmstart	(Optional) Enables warmstart traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to enable a warmstart SNMP trap:

```
Device(config)# snmp-server enable traps snmp warmstart
```

snmp-server enable traps stackwise

To enable SNMP StackWise traps, use the **snmp-server enable traps stackwise** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

no snmp-server enable traps stackwise [**GLS**][**ILS**][**SRLS**] [**insufficient-power**][**invalid-input-current**] [**invalid-output-current**][**member-removed**][**member-upgrade-notification**] [**new-master**][**new-member**] [**port-change**][**power-budget-warning**][**power-invalid-topology**] [**power-link-status-changed**][**power-oper-status-changed**] [**power-priority-conflict**][**power-version-mismatch**][**ring-redundant**] [**stack-mismatch**][**unbalanced-power-supplies**][**under-budget**][**under-voltage**]

Syntax Description

GLS	(Optional) Enables StackWise stack power GLS trap.
ILS	(Optional) Enables StackWise stack power ILS trap.
SRLS	(Optional) Enables StackWise stack power SRLS trap.
insufficient-power	(Optional) Enables StackWise stack power unbalanced power supplies trap.

invalid-input-current	(Optional) Enables StackWise stack power invalid input current trap.
invalid-output-current	(Optional) Enables StackWise stack power invalid output current trap.
member-removed	(Optional) Enables StackWise stack member removed trap.
member-upgrade-notification	(Optional) Enables StackWise member to be reloaded for upgrade trap.
new-master	(Optional) Enables StackWise new master trap.
new-member	(Optional) Enables StackWise stack new member trap.
port-change	(Optional) Enables StackWise stack port change trap.
power-budget-warning	(Optional) Enables StackWise stack power budget warning trap.
power-invalid-topology	(Optional) Enables StackWise stack power invalid topology trap.
power-link-status-changed	(Optional) Enables StackWise stack power link status changed trap.
power-oper-status-changed	(Optional) Enables StackWise stack power port oper status changed trap.
power-priority-conflict	(Optional) Enables StackWise stack power priority conflict trap.
power-version-mismatch	(Optional) Enables StackWise stack power version mismatch discovered trap.
ring-redundant	(Optional) Enables StackWise stack ring redundant trap.
stack-mismatch	(Optional) Enables StackWise stack mismatch trap.
unbalanced-power-supplies	(Optional) Enables StackWise stack power unbalanced power supplies trap.
under-budget	(Optional) Enables StackWise stack power under budget trap.
under-voltage	(Optional) Enables StackWise stack power under voltage trap.

Command Default

The sending of SNMP StackWise traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate StackWise stack power GLS traps:

```
Device(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps storm-control {**trap-rate** *number-of-minutes*}

no snmp-server enable traps storm-control {**trap-rate**}

Syntax Description

trap-rate *number-of-minutes*	(Optional) Specifies the SNMP storm-control trap rate in minutes. Accepted values are from 0 to 1000.

Command Default

The sending of SNMP storm-control trap parameters is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps stpx [**inconsistency**][**loop-inconsistency**][**root-inconsistency**]

no snmp-server enable traps stpx [**inconsistency**][**loop-inconsistency**][**root-inconsistency**]

Syntax Description

inconsistency	(Optional) Enables SNMP STPX MIB inconsistency update traps.
loop-inconsistency	(Optional) Enables SNMP STPX MIB loop inconsistency update traps.
root-inconsistency	(Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default

The sending of SNMP STPX MIB traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps transceiver {**all**}

no snmp-server enable traps transceiver {**all**}

Syntax Description

all	(Optional) Enables all SNMP transceiver traps.

Command Default

The sending of SNMP transceiver traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to set all SNMP transceiver traps:

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

To allow SNMP vrfmib traps, use the **snmp-server enable traps vrfmib** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

Syntax Description

vnet-trunk-down	(Optional) Enables vrfmib trunk down traps.
vnet-trunk-up	(Optional) Enables vrfmib trunk up traps.
vrf-down	(Optional) Enables vrfmib vrf down traps.
vrf-up	(Optional) Enables vrfmib vrf up traps.

Command Default

The sending of SNMP vrfmib traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate vrfmib trunk down traps:

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

To enable SNMP smart install traps, use the **snmp-server enable traps vstack** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vstack [**addition**][**failure**][**lost**][**operation**]

no snmp-server enable traps vstack [**addition**][**failure**][**lost**][**operation**]

Syntax Description

addition	(Optional) Enables client added traps.
failure	(Optional) Enables file upload and download failure traps.
lost	(Optional) Enables client lost trap.
operation	(Optional) Enables operation mode change traps.

Command Default

The sending of SNMP smart install traps is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

This example shows how to generate SNMP Smart Install client-added traps:

```
Device(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

To configure a name for either the local or remote copy of SNMP, use the **snmp-server engineID** command in global configuration mode.

snmp-server engineID {**local** *engineid-string* | **remote** *ip-address* [**udp-port** *port-number*] *engineid-string*}

Syntax Description

local *engineid-string*	Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.
remote *ip-address*	Specifies the remote SNMP copy. Specify the *ip-address* of the device that contains the remote copy of SNMP.
udp-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

Examples

The following example configures a local engine ID of 12340000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```

snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the device. Use the **no** form of this command to remove the specified host.

snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

no snmp-server host {*host-addr* } [**vrf** *vrf-instance*] [**informs** | **traps**] [**version** {**1** | **2c** | **3** {**auth** | **noauth** | **priv**} }] {*community-string* [*notification-type*] }

Syntax Description

host-addr	Name or Internet address of the host (the targeted recipient).
vrf *vrf-instance*	(Optional) Specifies the virtual private network (VPN) routing instance and name for this host.
informs | **traps**	(Optional) Sends SNMP traps or informs to this host.
version 1 | **2c** | **3**	(Optional) Specifies the version of the SNMP used to send the traps. **1**—SNMPv1. This option is not available with informs. **2c**—SNMPv2C. **3**—SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.
auth | **noauth** | **priv**	**auth** (Optional)—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication. **noauth** (Default)—The noAuthNoPriv security level. This is the default if the **auth** | **noauth** | **priv** keyword choice is not specified. **priv** (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).
community-string	Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. **Note** The @ symbol is used for delimiting the context information. Avoid using the @ symbol as part of the SNMP community string when configuring this command.

notification-type (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- **auth-framework—**Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
- **bridge—**Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
- **bulkstat—**Sends Data-Collection-MIB Collection notification traps.
- **call-home—**Sends SNMP CISCO-CALLHOME-MIB traps.
- **cef—**Sends SNMP CEF traps.
- **config—**Sends SNMP configuration traps.
- **config-copy—**Sends SNMP config-copy traps.
- **config-ctid—**Sends SNMP config-ctid traps.
- **copy-config—**Sends SNMP copy configuration traps.
- **cpu—**Sends CPU notification traps.
- **cpu threshold—**Sends CPU threshold notification traps.
- **eigrp—**Sends SNMP EIGRP traps.
- **entity—**Sends SNMP entity traps.

- **envmon—**Sends environmental monitor traps.
- **errdisable—**Sends SNMP errdisable notification traps.
- **event-manager—**Sends SNMP Embedded Event Manager traps.
- **flash—**Sends SNMP FLASH notifications.
- **flowmon—**Sends SNMP flowmon notification traps.
- **ipmulticast—**Sends SNMP IP multicast routing traps.
- **ipsla—**Sends SNMP IP SLA traps.
- **isis—**Sends IS-IS traps.
- **license—**Sends license traps.
- **local-auth—**Sends SNMP local auth traps.
- **mac-notification—**Sends SNMP MAC notification traps.
- **ospf—**Sends Open Shortest Path First (OSPF) traps.
- **pim—**Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **port-security—**Sends SNMP port-security traps.
- **power-ethernet—**Sends SNMP power Ethernet traps.
- **snmp—**Sends SNMP-type traps.
- **storm-control—**Sends SNMP storm-control traps.
- **stpx—**Sends SNMP STP extended MIB traps.
- **syslog—**Sends SNMP syslog traps.
- **transceiver—**Sends SNMP transceiver traps.
- **tty—**Sends TCP connection traps.
- **vlan-membership—** Sends SNMP VLAN membership traps.
- **vlancreate—**Sends SNMP VLAN-created traps.
- **vlandelete—**Sends SNMP VLAN-deleted traps.
- **vrfmib—**Sends SNMP vrfmib traps.
- **vstack—**Sends SNMP Smart Install traps.
- **vtp—**Sends SNMP VLAN Trunking Protocol (VTP) traps.
- **wireless—**Sends wireless traps.

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

Note Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

This example shows how to configure a unique SNMP community string named comaccess for traps and prevent SNMP polling access with this string through access-list 10:

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the device to send all traps to the host myhost.cisco.com by using the community string public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

switchport mode access

To sets the interface as a nontrunking nontagged single-VLAN Ethernet interface , use the **switchport mode access** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport mode access

no switchport mode access

Syntax Description

switchport mode access	Sets the interface as a nontrunking nontagged single-VLAN Ethernet interface.

Command Default

An access port can carry traffic in one VLAN only. By default, an access port carries traffic for VLAN1.

Command Modes

Template configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This example shows how to set a single-VLAN interface

```
Device(config-template)# switchport mode access
```

switchport voice vlan

To specify to forward all voice traffic through the specified VLAN, use the **switchport voice vlan** command in template configuration mode. Use the **no** form of this command to return to the default setting.

switchport voice vlan*vlan_id*

no switchport voice vlan

Syntax Description

switchport voice vlan*vlan_id*	Specifies to forward all voice traffic through the specified VLAN.

Command Default

You can specify a value from 1 to 4094.

Command Modes

Template configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Device(config-template)# switchport voice vlan 20
```

PART X

QoS

- QoS Commands, page 589

CHAPTER 11

QoS Commands

This chapter contains the following QoS commands:

- class, page 590
- class-map, page 592
- match (class-map configuration), page 593
- match non-client-nrt, page 596
- match wlan user-priority, page 597
- policy-map, page 597
- priority, page 599
- queue-buffers ratio, page 601
- queue-limit, page 603
- service-policy (Wired), page 604
- service-policy (WLAN), page 605
- set, page 606
- show ap name service-policy, page 612
- show ap name dot11, page 613
- show class-map, page 615
- show platform hardware fed switch, page 616
- show platform software fed switch qos, page 619
- show platform software fed switch qos qsb, page 620
- show wireless client calls, page 622
- show wireless client dot11, page 623
- show wireless client mac-address (Call Control), page 624
- show wireless client mac-address (TCLAS), page 625

- show wireless client voice diagnostics, page 625
- show policy-map, page 626
- show wlan, page 628
- trust device, page 630

class

To define a traffic classification match criteria for the specified class-map name, use the **class** command in policy-map configuration mode. Use the **no** form of this command to delete an existing class map.

class {*class-map-name* | **class-default**}

no class {*class-map-name* | **class-default**}

Syntax Description

class-map-name	The class map name.
class-default	Refers to a system default class that matches unclassified packets.

Command Default

No policy map class-maps are defined.

Command Modes

Policy-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before using the **class** command, you must use the **policy-map** global configuration command to identify the policy map and enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter the policy-map class configuration mode. These configuration commands are available:

- **admit—**Admits a request for Call Admission Control (CAC)
- **bandwidth—**Specifies the bandwidth allocated to the class.
- **exit—**Exits the policy-map class configuration mode and returns to policy-map configuration mode.
- **no—**Returns a command to its default setting.

- **police**—Defines a policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.
- **priority**—Assigns scheduling priority to a class of traffic belonging to a policy map.
- **queue-buffers**—Configures the queue buffer for the class.
- **queue-limit**—Specifies the maximum number of packets the queue can hold for a class policy configured in a policy map.
- **service-policy**—Configures a QoS service policy.
- **set**—Specifies a value to be assigned to the classified traffic. For more information, see set, on page 606
- **shape**—Specifies average or peak rate traffic shaping. For more information about this command, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

The **class** command performs the same function as the **class-map** global configuration command. Use the **class** command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

You can configure a default class by using the **class class-default** policy-map configuration command. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

You can verify your settings by entering the **show policy-map** privileged EXEC command.

This example shows how to create a policy map called policy1. When attached to the ingress direction, it matches all the incoming traffic defined in class1, sets the IP Differentiated Services Code Point (DSCP) to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic exceeding the profile is marked down to a DSCP value gotten from the policed-DSCP map and then sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit
```

```
Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
    set dscp af11
```

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

class-map [**match-any**| *type*] *class-map-name*

no class-map [**match-any**| *type*] *class-map-name*

Syntax Description

match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
type	(Optional) Configures the CPL class map.
class-map-name	The class map name.

Command Default

No class maps are defined.

Command Modes

Global configuration

Policy map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **type** keyword was added.

Usage Guidelines

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The **class-map** command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description—**Describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit—**Exits from QoS class-map configuration mode.
- **match—**Configures classification criteria.
- **no—**Removes a match statement from a class map.

If you enter the **match-any** keyword, you can only use it to specify an extended named access control list (ACL) with the **match access-group** class-map configuration command.

To define packet classification on a physical-port basis, only one **match** command per class map is supported.

The ACL can have multiple access control entries (ACEs).

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

match {**access-group**{**name***acl-name* | *acl-index*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

no match {**access-group**{**name***acl-name* | *acl-index*}| **class-map** *class-map-name*| **cos** *cos-value*| **dscp** *dscp-value*| **[ip] dscp** *dscp-list* | **[ip] precedence** *ip-precedence-list*| **precedence** *precedence-value1...value4*| **qos-group** *qos-group-value*| **vlan** *vlan-id*}

Syntax Description

access-group	Specifies an access group.

name *acl-name*	Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
acl-index	Specifies the number of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699.
class-map *class-map-name*	Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos *cos-value*	Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one **match cos** statement, separated by a space.
dscp *dscp-value*	Specifies the parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value.
ip dscp *dscp-list*	Specifies a list of up to eight IP Differentiated Services Code Point (DSCP) values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You also can enter a mnemonic name for a commonly used value.
ip precedence *ip-precedence-list*	Specifies a list of up to eight IP-precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
precedence *precedence-value1...value4*	Assigns an IP precedence value to the classified traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value.
qos-group *qos-group-value*	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan *vlan-id*	Identifies a specific VLAN as a match criterion. The range is 1 to 4095.

Command Default

No match criteria are defined.

Command Modes

Class-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **class-map** *class-map-name*, **cos** *cos-value*, **qos-group** *qos-group-value*, and **vlan** *vlan-id* keywords were added.

Usage Guidelines

The **match** command is used to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching to the Ether Type/Len are supported.

If you enter the **class-map match-any***class-map-name* global configuration command, you can enter the following **match** commands:

- **match access-group name** *acl-name*

Note The ACL must be an extended named ACL.

- **match ip dscp** *dscp-list*
- **match ip precedence** *ip-precedence-list*

The **match access-group** *acl-index* command is not supported.

To define packet classification on a physical-port basis, only one **match** command per class map is supported. In this situation, the **match-any** keyword is equivalent.

For the **match ip dscp** *dscp-list* or the **match ip precedence** *ip-precedence-list* command, you can enter a mnemonic name for a commonly used value. For example, you can enter the **match ip dscp af11** command, which is the same as entering the **match ip dscp 10** command. You can enter the **match ip precedence critical** command, which is the same as entering the **match ip precedence 5** command. For a list of supported mnemonics, enter the **match ip dscp ?** or the **match ip precedence ?** command to see the command-line help strings.

Use the **input-interface** *interface-id-list* keyword when you are configuring an interface-level class map in a hierarchical policy map. For the *interface-id-list*, you can specify up to six entries.

This example shows how to create a class map called class2, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match non-client-nrt

no match non-client-nrt

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

match wlan user-priority

To match 802.11 specific values, use the **match wlan user-priority** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

no match wlan user-priority *wlan-value* [*wlan-value*] [*wlan-value*] [*wlan-value*]

Syntax Description

wlan-value	The 802.11-specific values. Enter the user priority 802.11 TID user priority (0-7). (Optional) Enter up to three user priority values separated by white-spaces.

Command Default

None

Command Modes

Class-map

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None

This example show how you can configure user-priority values:

```
Device(config)# class-map test_1000
Device(config-cmap)# match wlan user-priority 7
```

policy-map

To create or modify a policy map that can be attached to multiple physical ports or switch virtual interfaces (SVIs) and to enter policy-map configuration mode, use the **policy-map** command in global configuration mode. Use the **no** form of this command to delete an existing policy map and to return to global configuration mode.

policy-map *policy-map-name*

no policy-map *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map.

Command Default

No policy maps are defined.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class—**Defines the classification match criteria for the specified class map.
- **description—**Describes the policy map (up to 200 characters).
- **exit—**Exits policy-map configuration mode and returns you to global configuration mode.
- **no—**Removes a previously defined policy map.
- **sequence-interval—**Enables sequence number capability.

To return to global configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created, added to, or modified. Entering the **policy-map** command also enables the policy-map configuration mode in which you can configure or modify the class policies for that policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

Only one policy map per ingress port is supported. You can apply the same policy map to multiple physical ports.

You can apply a nonhierarchical policy maps to physical ports. A nonhierarchical policy map is the same as the port-based policy maps in the device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be configured to refer to the VLAN-based policy maps instead of the port-based policy map.

Note Not all MQC QoS combinations are supported for wired and wireless ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired Targets" and "Restrictions for QoS on Wireless Targets" in the QoS configuration guide.

This example shows how to create a policy map called policy1. When attached to the ingress port, it matches all the incoming traffic defined in class1, sets the IP DSCP to 10, and polices the traffic at an average rate of 1 Mb/s and bursts at 20 KB. Traffic less than the profile is sent.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Switch# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Deviceconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

priority [*Kbps* [*burst -in-bytes*] | **level** *level-value* [*Kbps* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

no priority [*Kb/s* [*burst -in-bytes*] | **level** *level value* [*Kb/s* [*burst -in-bytes*]] | **percent** *percentage* [*Kb/s* [*burst -in-bytes*]]]

Syntax Description

Kb/s	(Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.
burst -in-bytes	(Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
level *level-value*	(Optional) Assigns priority level. Available values for *level-value* are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low. Reserve the bandwidth even if you do not use it. Both levels 1 and 2 can reserve bandwidth.
percent *percentage*	(Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

Command Default

No priority is set.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The *Kbps*, *burst -in-bytes*, and **percent** *percentage* keywords were added.

Usage Guidelines

This command configures low latency queuing (LLQ), providing strict priority queuing (PQ) for class-based weighted fair queuing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

Note You can configure a priority only with a level.
Only one strict priority or priority with levels is allowed in one policy-map. Multiple priorities with same priority levels without kbps/percent are allowed in a policy-map only if all of them are configured with police.

The priority command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **ip rtp priority** command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The bandwidth and priority commands cannot be used in the same class, within the same policy map. However, these commands can be used together in the same policy map.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

Example

The following example shows how to configure the priority of the class in policy map policy1:

```
Device(config)# class-map cm1
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#exit

Device(config)#policy-map policy1
Device(config-pmap)#class cm2
Device(config-pmap-c)#priority level 2
Device(config-pmap-c)#police 1m
```

queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

queue-buffers ratio *ratio limit*

no queue-buffers ratio *ratio limit*

Syntax Description

ratio limit	(Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).

Command Default

No queue buffer for the class is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com

The allows you to allocate buffers to queues. If buffers are not allocated, then they are divided equally amongst all queues. You can use the queue-buffer ratio to divide it in a particular ratio. The buffers are soft buffers because Dynamic Threshold and Scaling (DTS) is active on all queues by default.

Note The queue-buffer ratio is supported on both wired and wireless ports, but the queue-buffer ratio cannot be configured with a queue-limit.

Example

The following example sets the queue buffers ratio to 10 percent:

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
Device(config-pmap)# end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

queue-limit *queue-limit-size* [**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

no queue-limit *queue-limit-size* [**packets**] {**cos** *cos-value*| **dscp** *dscp-value*} **percent** *percentage-of-packets*

Syntax Description

queue-limit-size	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
cos *cos-value*	Specifies parameters for each cos value. CoS values are from 0 to 7.
dscp *dscp-value*	Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit .
percent *percentage-of-packets*	A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

Command Default

None

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Although visible in the command line help-strings, the **packets** unit of measure is not supported; use the **percent** unit of measure.

Note This command is supported only on wired ports in the egress direction.

Weighted fair queuing (WFQ) creates a queue for every class for which a class map is defined. Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queuing process. When the maximum packet threshold you defined for the class is reached, queuing of any further packets to the class queue causes tail drop.

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation.

You can configure the maximum queue thresholds for the different subclasses of traffic, that is, DSCP and CoS and configure the maximum queue thresholds for each subclass.

Example

The following example configures a policy map called port-queue to contain policy for a class called dscp-1. The policy for this class is set so that the queue reserved for it has a maximum packet limit of 20 percent:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

service-policy {**input** | **output**} *policy-map-name*

no service-policy {**input** | **output**} *policy-map-name*

Syntax Description

input *policy-map-name*	Apply the specified policy map to the input of a physical port or an SVI.
output *policy-map-name*	Apply the specified policy map to the output of a physical port or an SVI.

Command Default

No policy maps are attached to the port.

Command Modes

WLAN interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI. *QoS Configuration Guide (Catalyst 3850 Switches)*.

Note Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

This example shows how to apply plcmap1 to an physical ingress port:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)#  service-policy input vlan100
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [client] {**input**| **output**} *policy-name*

no service-policy [client] {**input**| **output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.

output	Assigns an output policy map.
policy-name	The policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

Related Topics

wlan, on page 1022

wlan, on page 1022

set

To classify IP traffic by setting a Differentiated Services Code Point (DSCP) or an IP-precedence value in the packet, use the **set** command in policy-map class configuration mode. Use the **no** form of this command to remove traffic classification.

set cos| dscp| precedence| ip| qos-group| wlan

set cos {*cos-value* } | {**cos**| **dscp**| **precedence**| **qos-group**| **wlan**} [**table** *table-map-name*]

set dscp {*dscp-value* } | {**cos**| **dscp**| **precedence**| **qos-group**| **wlan**} [**table** *table-map-name*]

set ip {**dscp**| **precedence**}

set precedence {*precedence-value* } | {**cos**| **dscp**| **precedence**| **qos-group**} [**table** *table-map-name*]

set qos-group {*qos-group-value*| **dscp** [**table** *table-map-name*]| **precedence** [**table** *table-map-name*]}

set wlan user-priority*user-priority-value*| **costable** *table-map-name*| **dscptable** *table-map-name*| **qos-grouptable** *table-map-name*| **wlantable** *table-map-name*

Syntax Description

cos

Sets the Layer 2 class of service (CoS) value or user priority of an outgoing packet. You can specify these values:

- *cos-value*—CoS value from 0 to 7. You also can enter a mnemonic name for a commonly used value.
- Specify a packet-marking category to set the CoS value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords:
  - **cos**—Sets a value from the CoS value or user priority.
  - **dscp**—Sets a value from packet differentiated services code point (DSCP).
  - **precedence**—Sets a value from packet precedence.
  - **qos-group**—Sets a value from the QoS group.
  - **wlan**—Sets the WLAN user priority values.
- (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map are used to set the CoS value. Enter the name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters.

  If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence (packet-marking category) value is copied and used as the CoS value.

dscp	Sets the differentiated services code point (DSCP) value to mark IP(v4) and IPv6 packets. You can specify these values: • *cos-value*—Number that sets the DSCP value. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value. • Specify a packet-marking category to set the DSCP value of the packet. If you also configure a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords: ◦ **cos**—Sets a value from the CoS value or user priority. ◦ **dscp**—Sets a value from packet differentiated services code point (DSCP). ◦ **precedence**—Sets a value from packet precedence. ◦ **qos-group**—Sets a value from the QoS group. ◦ **wlan**—Sets a value from WLAN. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP value. Enter the name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value (packet-marking category) is copied and used as the DSCP value.
ip	Sets IP values to the classified traffic. You can specify these values: • **dscp**—Specify an IP DSCP value from 0 to 63 or a packet marking category. • **precedence**—Specify a precedence-bit value in the IP header; valid values are from 0 to 7 or specify a packet marking category.

precedence	Sets the precedence value in the packet header. You can specify these values: • *precedence-value*— Sets the precedence bit in the packet header; valid values are from 0 to 7. You also can enter a mnemonic name for a commonly used value. • Specify a packet marking category to set the precedence value of the packet. ◦ **cos**—Sets a value from the CoS or user priority. ◦ **dscp**—Sets a value from packet differentiated services code point (DSCP). ◦ **precedence**—Sets a value from packet precedence. ◦ **qos-group**—Sets a value from the QoS group. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the precedence value. Enter the name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value (packet-marking category) is copied and used as the precedence value.

qos-group	Assigns a QoS group identifier that can be used later to classify packets. • *qos-group-value*—Sets a QoS value to the classified traffic. The range is 0 to 31. You also can enter a mnemonic name for a commonly used value. • **dscp**—Sets the original DSCP field value of the packet as the QoS group value. • **precedence**—Sets the original precedence field value of the packet as the QoS group value. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the DSCP or precedence value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category (**dscp** or **precedence**) but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the QoS group value. For example, if you enter the **set qos-group precedence** command, the precedence value (packet-marking category) is copied and used as the QoS group value.

wlan user-priority *wlan-user-priority*	Assigns a WLAN user-priority to the classified traffic. You can specify these values: • *wlan-user-priority*—Sets a WLAN user priority to the classified traffic. The range is 0 to 7. • **cos**—Sets the Layer 2 CoS field value as the WLAN user priority. • **dscp**—Sets the DSCP field value as the WLAN user priority. • **precedence**—Sets the precedence field value as the WLAN user priority. • **wlan**—Sets the WLAN user priority field value as the WLAN user priority. • (Optional)**table** *table-map-name*—Indicates that the values set in a specified table map will be used to set the WLAN user priority value. Enter the name of the table map used to specify the value. The table map name can be a maximum of 64 alphanumeric characters. If you specify a packet-marking category but do not specify the table map, the default action is to copy the value associated with the packet-marking category as the WLAN user priority. For example, if you enter the **set wlan user-priority cos** command, the cos value (packet-marking category) is copied and used as the WLAN user priority.

Command Default

No traffic classification is defined.

Command Modes

Policy-map class configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **cos**, **dscp**, **qos-group**, **wlantable** *table-map-name*, keywords were added.

Usage Guidelines

For the **set dscp** *dscp-value* command, the **set cos** *cos-value* command, and the **set ip precedence** *precedence-value* command, you can enter a mnemonic name for a commonly used value. For example, you

can enter the **set dscp af11** command, which is the same as entering the **set dscp 10** command. You can enter the **set ip precedence critical** command, which is the same as entering the **set ip precedence 5** command. For a list of supported mnemonics, enter the **set dscp ?** or the **set ip precedence ?** command to see the command-line help strings.

When you configure the **set dscp cos**command, note the following: The CoS value is a 3-bit field, and the DSCP value is a 6-bit field. Only the three bits of the CoS field are used.

When you configure the **set dscp qos-group** command, note the following:

- The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99.
- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value is copied and the packets is marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value is not be copied and the packet is not marked. No action is taken.

The **set qos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

show ap name service-policy

To display service-policy information for a specific Cisco lightweight access point, use the **show ap name service-policy** command.

show ap name *ap-name* **service-policy**

Syntax Description

ap-name	Name of the Cisco lightweight access point.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display service-policy information for a specific Cisco lightweight access point:

```
Device# show ap name 3502b service-policy

NAME: Cisco AP    , DESCR: Cisco Wireless Access Point
PID: 3502I  ,  VID: V01,  SN: FTX1525E94A


NAME: Dot11Radio0    , DESCR: 802.11N 2.4GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA


NAME: Dot11Radio1    , DESCR: 802.11N 5GHz Radio
PID: UNKNOWN,  VID:  ,  SN: FOC1522BLNA
```

show ap name dot11

To display 802.11a or 802.11b configuration information that corresponds to specific Cisco lightweight access points, use the **show ap name dot11** command.

show ap name *ap-name* **dot11** {**24ghz**| **5ghz**} {**ccx**| **cdp**| **profile**| **service-poicy output**| **stats**| **tsm** {**all**| *client-mac*}}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
24ghz	Displays the 2.4 GHz band.
5ghz	Displays the 5 GHz band.
ccx	Displays the Cisco Client eXtensions (CCX) radio management status information.
cdp	Displays Cisco Discovery Protocol (CDP) information.
profile	Displays configuration and statistics of 802.11 profiling.
service-policy output	Displays downstream service policy information.
stats	Displays Cisco lightweight access point statistics.
tsm	Displays 802.11 traffic stream metrics statistics.
all	Displays the list of all access points to which the client has associations.
client-mac	MAC address of the client.

Command Default None

Command Modes Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the service policy that is associated with the access point:

```
Device# show ap name test-ap dot11 24ghz service-policy output

Policy Name  : test-ap1
Policy State : Installed
```

This example shows how to display the CCX RRM 802.11 configuration for a specific access point:

```
Device# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz cdp

AP Name               AP CDP State
--------------------- --------------
AP03                  Disabled
```

This example show how to display the configuration and statistics of 802.11b profiling for a specific access point:

```
Device# show ap name AP01 dot11 24ghz profile

 802.11b Cisco AP performance profile mode            : GLOBAL
 802.11b Cisco AP Interference threshold              : 10 %
 802.11b Cisco AP noise threshold                     : -70 dBm
 802.11b Cisco AP RF utilization threshold            : 80 %
 802.11b Cisco AP throughput threshold                : 1000000 bps
 802.11b Cisco AP clients threshold                   : 12 clients
```

This example show how to display downstream service policy information for a specific access point:

```
Device# show ap name AP01 dot11 24ghz service-policy output

Policy Name  : def-11gn
Policy State : Installed
```

This example show how to display statistics for a specific access point:

```
Device# show ap name AP01 dot11 24ghz stats

Number of Users................................: 0
TxFragmentCount................................: 0
MulticastTxFrameCnt............................: 0
FailedCount....................................: 0
RetryCount.....................................: 0
MultipleRetryCount.............................: 0
FrameDuplicateCount............................: 0
RtsSuccessCount................................: 0
RtsFailureCount................................: 0
```

```
AckFailureCount.............................: 0
RxIncompleteFragment........................: 0
MulticastRxFrameCnt.........................: 0
FcsErrorCount...............................: 0
TxFrameCount................................: 0
WepUndecryptableCount.......................: 0
TxFramesDropped.............................: 0

Call Admission Control (CAC) Stats
  Voice Bandwidth in use(% of config bw)........: 0
  Video Bandwidth in use(% of config bw)........: 0
  Total BW in use for Voice(%)..................: 0
  Total BW in use for SIP Preferred call(%)......: 0

Load based Voice Call Stats
  Total channel MT free........................: 0
  Total voice MT free..........................: 0
  Na Direct....................................: 0
  Na Roam......................................: 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

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
```

This example show how to display the traffic stream configuration for all clients that correspond to a specific access point:

```
Device# show ap name AP01 dot11 24ghz tsm all
```

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

show class-map [*class-map-name* | **type control subscriber** {**all** | *class-map-name*}]

Syntax Description

class-map-name	(Optional) Class map name.
type control subscriber	(Optional) Displays information about control class maps.
all	(Optional) Displays information about all control class maps.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show class-map** command:

```
Device# show class-map
 Class Map match-any videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any dscp5 (id 3)
   Match ip dscp 5
```

show platform hardware fed switch

To display device-specific hardware information, use the **show platform hardware fed switch***switch_number* command.

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform hardware fed switch {*switch_num*| **active**| **standby**} **qos** {**afd** | {**config type** *type* | [**asic** *asic_num*]| **stats clients** {**all**| **bssid** *id*| **wlanid** *id* }}| **dscp-cos counters** {**iifd_id** *id*| **interface***type number*}| **le-info** | {**iifd_id** *id*| **interface** *type number*}| **policer config** {**iifd_id** *id*| **interface** *type number*}| **queue** | {**config** | {**iifd_id** *id*| **interface** *type number*| **internal port-type** *type* {**asic** *number* [**port_num**]}}| **label2qmap** | [**aqmrepqostbl**| **iqslabeltable**| **sqslabeltable**]| {**asic***number*}| **stats** | {**iifd_id** *id*| **interface** *type number*| **internal** {**cpu policer**| **port-type** *type* **asic** *number*}{**asic***number* [**port_num**]}}}| **resource**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	Switch for which you want to display information. You have the following options: • *switch_num*—ID of the switch. • **active**—Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available.
qos	Displays QoS hardware information. You must choose from the following options: • **afd** —Displays Approximate Fair Drop (AFD) information in hardware. • **dscp-cos**—Displays information dscp-cos counters for each port. • **leinfo**—Displays logical entity information. • **policer**—Displays QoS policer information in hardware. • **queue**—Displays queue information in hardware. • **resource**—Displays hardware resource information.
afd {**config type** | **stats client** }	You must choose from the options under **config type** or **stats client** : **config type**: • **client**—Displays wireless client information • **port**—Displays port-specific information • **radio**—Displays wireless radio information • **ssid**—Displays wireless SSID information **stats client** : • **all**—Displays statistics of all client. • **bssid**—Valid range is from 1 to 4294967295. • **wlanid**—Valid range is from to 1 4294967295
asic*asic_num*	(Optional) ASIC number. Valid range is from 0 to 255.
dscp-cos counters { **iifd_id** *id* | **interface** *type number* }	Displays per port dscp-cos counters. You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.
leinfo	You must choose from the following options under **dscp-cos counters**: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.

policer config	Displays configuration information related to policers in hardware. You must choose from the following options: • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295. • **interface** *type number*—Target interface type and ID.

queue {**config** {**iif_id** *id* | **interface** *type number* | **internal**} | **label2qmap** | **stats**}	Displays queue information in hardware. You must choose from the following options:
	• **config**—Configuration information. You must choose from the following options:
	  • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295.
	  • **interface** *type number*—Target interface type and ID.
	  • **internal**—Displays internal queue related information.
	• **label2qmap**—Displays hardware label to queue mapping information. You can choose from the following options:
	  • (Optional) **aqmrepqostbl**— AQM REP QoS label table lookup.
	  • (Optional) **iqslabeltable**—IQS QoS label table lookup.
	  • (Optional) **sqslabeltable**—SQS and local QoS label table lookup.
	• **stats**—Displays queue statistics. You must choose from the following options:
	  • **iif_id** *id*—The target interface ID. Valid range is from 1 to 4294967295.
	  • **interface** *type number*—Target interface type and ID.
	  • **internal** {**cpu policer** | **port_type** *port_type* **asic** *asic_num* [**port_num** *port_num*] }—Displays internal queue related information.

resource	Displays hardware resource usage information. You must enter the following keyword: **usage**

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the**show platform hardware fed switch***switch_number***qos queue stats internal cpu policer** command

```
Device#show platform hardware fed switch 3 qos queue stats internal cpu policer

                                                (default)  (set)
QId PlcIdx  Queue Name                 Enabled   Rate     Rate      Drop
----------------------------------------------------------------------------
0    11     DOT1X Auth                  No      1000      1000        0
1    1      L2 Control                  No      500       500         0
2    14     Forus traffic               No      1000      1000        0
3    0      ICMP GEN                    Yes     200       200         0
4    2      Routing Control             Yes     1800      1800        0
5    14     Forus Address resolution    No      1000      1000        0
6    3      ICMP Redirect               No      500       500         0
7    6      WLESS PRI-5                 No      1000      1000        0
8    4      WLESS PRI-1                 No      1000      1000        0
9    5      WLESS PRI-2                 No      1000      1000        0
10   6      WLESS PRI-3                 No      1000      1000        0
11   6      WLESS PRI-4                 No      1000      1000        0
12   0      BROADCAST                   Yes     200       200         0
13   10     Learning cache ovfl         Yes     100       100         0
14   13     Sw forwarding               Yes     1000      1000        0
15   8      Topology Control            No      13000     13000       0
16   12     Proto Snooping              No      500       500         0
17   16     DHCP Snooping               No      1000      1000        0
18   9      Transit Traffic             Yes     500       500         0
19   10     RPF Failed                  Yes     100       100         0
20   15     MCAST END STATION           Yes     2000      2000        0
21   13     LOGGING                     Yes     1000      1000        0
22   7      Punt Webauth                No      1000      1000        0
23   10     Crypto Control              Yes     100       100         0
24   10     Exception                   Yes     100       100         0
25   3      General Punt                No      500       500         0
26   10     NFL SAMPLED DATA            Yes     100       100         0
27   2      SGT Cache Full              Yes     1800      1800        0
28   10     EGR Exception               Yes     100       100         0
29   16     Show frwd                   No      1000      1000        0
30   9      MCAST Data                  Yes     500       500         0
31   10     Gold Pkt                    Yes     100       100         0
```

show platform software fed switch qos

To display device-specific software information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options available with the **show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform software fed switch {*switch number*| **active**| **standby**}**qos**{**avc** | **internal**| **label2qmap**| **nflqos**| **policer**| **policy**| **qsb**| **tablemap**| **wireless**}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The device for which you want to display information. • *switch_num*—Enter the switch ID. Displays information for the specified switch. • **active**—Displays information for the active switch. • **standby**—Displays information for the standby switch, if available.

qos	Displays QoS software information. Choose one the following options: • **avc —**Displays Application Visibility and Control (AVC) QoS information. • **internal—**Displays internal queue-related information. • **label2qmap—**Displays label to queue map table information. • **nflqos—**Displays NetFlow QoS information. • **policer—**Displays QoS policer information in hardware. • **policy—**Displays QoS policy information. • **qsb—**Displays QoS sub-block information. • **tablemap—**Displays table mapping information for QoS egress and ingress queues. • **wireless—**Displays wireless QoS information.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch** *switch_number* **qos qsb** command.

show platform software fed switch{*switch number*| **active**| **standby**}**qosqsb**{**brief**| [**all**| **type**| {**client**| *client_id*| **port** | *port_number*| **radio**| *radio_type*| **ssid**| *ssid*}]| **iif_id**| *id*| **interface**| {**Auto-Template**| *interface_number*| **BDI**| *interface_number*| **Capwap**| *interface_number*| **GigabitEthernet**| *interface_number*| **InternalInterface**| *interface_number*| **Loopback**| *interface_number*| **Null**| *interface_number*| **Port-channel**| *interface_number*| **TenGigabitEthernet**| *interface_number*| **Tunnel**| *interface_number*| **Vlan**| *interface_number*}}

Syntax Description

switch {*switch_num* | **active** | **standby** }	The switch for which you want to display information. • *switch_num*—Enter the ID of the switch. Displays information for the specified switch. • **active—**Displays information for the active switch. • **standby—**Displays information for the standby switch, if available.

qos qsb	Displays QoS sub-block software information.
qsb {**brief** | **iif_id** | **interface**}	**brief** • **all—**Displays information for all client. • **type—**Displays qsb information for the specified target type: ◦ **client—**Displays QoS qsb information for wireless clients ◦ **port—**Displays port-specific information ◦ **radio—**Displays QoS qsb information for wireless radios ◦ **ssid—**Displays QoS qsb information for wireless networks **iif_id—**Displays information for the iif_ID **interface—**Displays QoS qsb information for the specified interface: • **Auto-Template—**Auto-template interface between 1 and 999. • **BDI—**Bridge-domain interface between 1 and 16000. • **Capwap—**CAPWAP interface between 0 and 2147483647. • **GigabitEthernet—**GigabitEthernet interface between 0 and 9. • **InternalInterface—**Internal interface between 0 and 9. • **Loopback—**Loopback interface between 0 and 2147483647. • **Null—**Null interface 0-0 • **Port-Channel—**Port-channel interface between 1 and 128. • **TenGigabitEthernet—**TenGigabitEthernet interface between 0 and 9. • **Tunnel—**Tunnel interface between 0 and 2147483647. • **Vlan—**VLAN interface between 1 and 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

This is an example of the output for the**show platform software fed switch***switch_number***qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2

  QoS subblock information:
```

```
 Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
 qsb ptr:0xffd8573350
 Port type = Wired port
 asic_num:0 is_uplink:false init_done:true
 FRU events: Active-0, Inactive-0
 def_qos_label:0 def_le_priority:13
 trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
 LE priority:13 LE trans_index(in, out): (0,0)
 Stats (plc,q) export counters (in/out): 0/0
 Policy Info:
   Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,)}
    tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
   Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,)}
    tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
   TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
 Policer Info:
   num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
   num_mf_policers(in,out): (0,0)
   num_afd_policers:0
   [ag_plc_handle(in,out) = (0xd8688220,0)]
   [mf_plc_handle(in,out)=((nil),(nil)) num_mf_policers:(0,0)
     base:(0xffffffff,0xffffffff) rc:(0,0)]
 Queueing Info:
   def_queuing = 0, shape_rate:0 interface_rate_kbps:1000000
   Port shaper:false
   lbl_to_qmap_index:1
   Physical qparams:
    Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

       PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
       Queue Limit Type:Single Unit:Percent Queue Limit:44192
       SHARED Queue
```

show wireless client calls

To display the total number of active or rejected calls on the device, use the **show wireless client calls** command in privileged EXEC mode.

show wireless client calls {**active** | **rejected**}

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client calls** command:

```
device# show wireless client calls active

TSPEC Calls:

-----------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
-----------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated              1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command in privileged EXEC mode.

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

Syntax Description

24ghz	Displays the 802.11b/g network.
5ghz	Displays the 802.11a network.
calls	Displays the wireless client calls.
active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client dot11** command:

```
Device# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------
```

```
SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client mac-address (Call Control)

To view call control information related to clients, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **call-control call-info**

Syntax Description

mac-address	The client MAC address.
call-control call-info	Displays the call control and IP-related information about a client.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display call control and IP-related information about a client:

```
Device# show wireless client mac-address  30e4.db41.6157 call-control call-info
Client MAC Address        : 30E4DB416157

Call 1 Statistics

Uplink IP Address         : 209.165.200.225
Downlink IP Address       : 209.165.200.226
Uplink Port               : 29052
Downlink Port             : 27538
Call ID                   : c40acb4d-3b3b0.3d27da1e-356bed03
Called Party              : sip:1011
Calling Party             : sip:1012
Priority                  : 6
Call On Hold              : false
Call Duration             : 30

Call 2 Statistics

No Active Call
```

show wireless client mac-address (TCLAS)

To view information about TCLAS and user priority, use the **show wireless client mac-address** command in privileged EXEC mode.

show wireless client mac-address *mac-address* **tclas**

Syntax Description

mac-address	The client MAC address.
tclas	Displays TCLAS and user priority-related information about a client.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the TCLAS and user priority-related information about a client:

```
Device# show wireless client mac-address 30e4.db41.6157 tclas
MAC Address      UP TID Mask Source IP Addr  Dest IP Addr    SrcPort DstPort Proto
--------------------------------------------------------------------------------
30e4.db41.6157    4   4   95 167838052       2164326668      5060     5060      6
30e4.db41.6157    6   1   31 0               2164326668      0        27538    17
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command in privileged EXEC mode.

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

qos-map	Displays information about the QoS and 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 the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.

status	Displays status of voice diagnostics for clients.
tspec	Displays voice diagnostics that are enabled for TSPEC clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Debug voice diagnostics must be enabled for voice diagnostics to work.

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Device# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show policy-map

To display quality of service (QoS) policy maps, which define classification criteria for incoming traffic, use the **show policy-map** command in EXEC mode.

show policy-map [*policy-map-name*| **interface** *interface-id*]

show policy-map interface {**Auto-template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Lspvif** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan** | **brief** | **class** | **input** | **output**

show policy-map type control subscriber detail

show policy-map interface wireless {**ap name** *ap_name* | **client mac** *mac_address* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name* | **ssid name** *ssid_name* {**ap name** *ap_name* | **radio type** {**24ghz** | **5ghz**} **ap name** *ap_name*}}

Syntax Description

policy-map-name	(Optional) Name of the policy-map.
interface *interface-id*	(Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.
type control subscriber detail	(Optional) Identifies the type of QoS policy and the statistics.

ap name *ap_name*	Displays SSID policy configuration of an access point.
client mac *mac_address*	Displays information about the policies for all the client targets.
radio type {**24ghz** | **5ghz**	Displays policy configuration of the access point in the specified radio type.
ssid name *ssid_name*	Displays policy configuration of an SSID.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **interface** *interface-id* keyword was added.

Usage Guidelines

Policy maps can include policers that specify the bandwidth limitations and the action to take if the limits are exceeded.

Note Though visible in the command-line help string, the **control-plane**, **session**, and **type** keywords are not supported, and the statistics shown in the display should be ignored.

This is an example of the output for the **show policy-map interface** command.

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48

  Service-policy output: port_shape_parent

    Class-map: class-default (match-any)
      191509734 packets
      Match: any
      Queueing

      (total drops) 524940551420
      (bytes output) 14937264500
      shape (average) cir 250000000, bc 2500000, be 2500000
      target shape rate 250000000

      Service-policy : child_trip_play

        queue stats for all priority classes:
          Queueing
          priority level 1

          (total drops) 524940551420
          (bytes output) 14937180648

        queue stats for all priority classes:
          Queueing
          priority level 2
```

```
    (total drops) 0
    (bytes output) 0

  Class-map: dscp56 (match-any)
    191508445 packets
    Match:  dscp cs7 (56)
      0 packets, 0 bytes
      5 minute rate 0 bps
    Priority: Strict,

    Priority Level: 1
    police:
        cir 10 %
        cir 25000000 bps, bc 781250 bytes
      conformed 0 bytes; actions: >>>>>counters not supported
        transmit
      exceeded 0 bytes; actions:
        drop
      conformed 0000 bps, exceeded 0000 bps  >>>>>counters not supported
```

show wlan

To view WLAN parameters, use the **show wlan** command.

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

Syntax Description

all	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
id *wlan-id*	Specifies the wireless LAN identifier. The range is from 1 to 512.
name *wlan-name*	Specifies the WLAN profile name. The name is from 1 to 32 characters.
summary	Displays a summary of the parameters configured on a WLAN.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display a summary of the WLANs configured on the device:

```
Device# show wlan summary
Number of WLANs: 1
```

```
WLAN Profile Name                    SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                       test-wlan-ssid                  1    UP
```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Device# show wlan name test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
```

```
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
    Cranite Passthru                            : Disabled
    Fortress Passthru                           : Disabled
    PPTP                                        : Disabled
    Infrastructure MFP protection               : Enabled
    Client MFP                                  : Optional
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
    Tkip MIC Countermeasure Hold-down Timer     : 60
Call Snooping                                   : Disabled
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
IP Source Guard                                 : Disabled
Netflow Monitor                                 : test
        Direction                               : Input
        Traffic                                 : Datalink

Mobility Anchor List
IP Address
-----------
```

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

no trust device {**cisco-phone** | **cts** | **ip-camera** | **media-player**}

Syntax Description

cisco-phone	Configures a Cisco IP phone
cts	Configures a Cisco TelePresence System
ip-camera	Configures an IP Video Surveillance Camera (IPVSC)
media-player	Configures a Cisco Digital Media Player (DMP)

Command Default

Trust disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **trust device** command on the following types of interfaces:

- **Auto—** auto-template interface
- **Capwap—**CAPWAP tunnel interface
- **GigabitEthernet—**Gigabit Ethernet IEEE 802
- **GroupVI—**Group virtual interface
- **Internal Interface—**Internal interface
- **Loopback—**Loopback interface
- **Null—**Null interface
- **Port-channel—**Ethernet Channel interface
- **TenGigabitEthernet--**10-Gigabit Ethernet
- **Tunnel—**Tunnel interface
- **Vlan—**Catalyst VLANs
- **range—interface range** command

Example

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Device(config)# interface GigabitEthernet1/0/1
Device(config-if)# trust device cisco-phone
```

You can verify your settings by entering the **show interface status** privileged EXEC command.

PART XI

Radio Resource Management

- Radio Resource Management Commands, page 635

CHAPTER 12

Radio Resource Management Commands

- ap dot11 rrm, page 635
- ap dot11 rrm ccx, page 638
- ap dot11 rrm channel, page 638
- ap dot11 24ghz rrm channel cleanair-event rogue-contribution, page 639
- ap dot11 24ghz or 5ghz rrm channel dca add, page 640
- ap dot11 24ghz or 5ghz rrm channel dca remove, page 641
- ap dot11 5ghz rrm channel dca chan-width-11n, page 642
- ap dot11 rrm coverage, page 642
- ap dot11 rrm group-member, page 644
- ap dot11 rrm monitor, page 644
- ap dot11 rrm profile, page 645
- ap dot11 rrm tpc-threshold, page 646
- ap dot11 rrm txpower, page 647
- show ap dot11 24ghz , page 648
- show ap dot11 5ghz, page 649

ap dot11 rrm

To configure basic and advanced radio resource management settings for 802.11 devices, use the **ap dot11 rrm** command.

ap dot11 {**24ghz**| **5ghz**} **rrm** {**ccx location-measurement** *sec*| **channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**| **outdoor-ap-dca**}| **coverage** {**data fail-percentage** *pct*| **data packet-count** *count*| **data rssi-threshold** *threshold*}| **exception global** *percentage*| **level global** *number*| **voice** {**fail-percentage** *percentage*| **packet-count** *number*| **rssi-threshold** *threshold*}}

Syntax Description

ccx	Configures Advanced (RRM) 802.11 CCX options.
location-measurement	Specifies 802.11 CCX Client Location Measurements in seconds. The range is between 10 and 32400 seconds.
channel	Configure advanced 802.11-channel assignment parameters.
cleanair-event	Configures cleanair event-driven RRM parameters.
dca	Configures 802.11-dynamic channel assignment algorithm parameters.
device	Configures persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.
outdoor-ap-dca	Configures 802.11 DCA list option for outdoor AP.
coverage	Configures 802.11 coverage Hole-Detection.
data fail-percentage *pct*	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
data packet-count *count*	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.

data rssi-threshold *threshold*	Configures 802.11 minimum-receive-coverage level for voice packets.
exception global *percentage*	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *number*	Configures 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Configures 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Configures 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *number*	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Configures 802.11 minimum receive coverage level for voice packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command applies for both 802.11a and 802.11b bands. But the appropriate commands must be chosen for configuring the parameter.

This example shows how to configure various RRM settings.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ?
  ccx            Configure Advanced(RRM) 802.11a CCX options
  channel        Configure advanced 802.11a channel assignment parameters
  coverage       802.11a Coverage Hole Detection
  group-member   Configure members in 802.11a static RF group
```

```
group-mode     802.11a RF group selection mode
logging        802.11a event logging
monitor        802.11a statistics monitoring
ndp-type       Neighbor discovery type Protected/Transparent
profile        802.11a performance profile
tpc-threshold  Configures the Tx Power Control Threshold used by RRM for auto
               power assignment
txpower        Configures the 802.11a Tx Power Level
```

ap dot11 rrm ccx

To configure radio resource management CCX options for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm ccx** command.

ap dot11 {**24ghz**| **5ghz**} **rrm ccx location-measurement** *interval*

Syntax Description

location-measurement *interval*	Specifies the CCX client-location measurement interval value. The range is between 10 and 32400 seconds.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to set CCX location-measurement interval for a 5-GHz device.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm ccx location-measurement 10
```

ap dot11 rrm channel

To enable radio resource management channel for 2.4 GHz and 5GHz devices, use the **ap dot11 rrm channel** command. To disable the radio resource mangement for 2.4 GHz and 5 GHz devices, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

no ap dot11 {**24ghz**| **5ghz**} **rrm channel** {**cleanair-event**| **dca**| **device**| **foreign**| **load**| **noise**}

Syntax Description

cleanair-event	Specifies the cleanair event-driven RRM parameters
dca	Specifies the 802.11 dynamic channel assignment algorithm parameters
device	Specifies the persistent non-WiFi device avoidance in the 802.11-channel assignment.
foreign	Enables foreign AP 802.11-interference avoidance in the channel assignment.
load	Enables Cisco AP 802.11-load avoidance in the channel assignment.
noise	Enables non-802.11-noise avoidance in the channel assignment.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows all the parameters available for **Channel**.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz rrm channel ?
  cleanair-event  Configure cleanair event-driven RRM parameters
  dca             Config 802.11b dynamic channel assignment algorithm
                  parameters
  device          Configure persistent non-WiFi device avoidance in the 802.11b
                  channel assignment
  foreign         Configure foreign AP 802.11b interference avoidance in the
                  channel assignment
  load            Configure Cisco AP 802.11b load avoidance in the channel
                  assignment
  noise           Configure 802.11b noise avoidance in the channel assignment
```

ap dot11 24ghz rrm channel cleanair-event rogue-contribution

To configure cleanair event driven Radio Resource Management (RRM) rogue contribution parameters, use the **ap dot11 24ghz rrm channel cleanair-event rogue-contribution** command.

ap dot11 24ghz rrm channel cleanair-event rogue-contribution duty-cycle *threshold-value*

Syntax Description

duty-cycle	Sets event-driven RRM rogue contribution duty cycle.
threshold-value	Custom ED-RRM rogue contribution duty cycle threshold value. Valid value ranges from 1 -99 percent.

Command Default

The rogue contribution duty cycle is not set.

Command History

Release	Modification
16.1	This command was introduced.

Usage Guidelines

This command sets event-driven RRM rogue contribution duty cycle.

Example

This example shows how to configure cleanair event driven RRM rogue contribution parameters:

```
 Cisco Controller(config)# ap dot11 24ghz rrm channel cleanair-event rogue-contribution
duty-cycle 1
```

ap dot11 24ghz or 5ghz rrm channel dca add

To add non-default radio resource management DCA channels to the DCA channel list for 2.4 GHz or 5 GHz devices, use the **ap dot11** {**24ghz** | **5ghz** } **rrm channel dca add** command. To remove a default channel from the DCA list, use the **no** form of the command. The DCA channel list contains standard channels matching your country of operation. For example, a regulatory default channel list contains channels 1, 6, and 11.

ap dot11 [**24ghz**| **5ghz**] **rrm channel dca add** *number*

no ap dot11 [**24ghz**| **5ghz**] **rrm channel dca add** *number*

Syntax Description

number	DCA channel number.

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None.

This example shows how to add a non-default radio resource management DCA channel to the DCA list for a 2.4 GHz device, using the **ap dot11 24ghz rrm channel dca add 10** command:

```
Device(config)# ap dot11 24ghz rrm channel dca add 10
```

ap dot11 24ghz or 5ghz rrm channel dca remove

To remove a default radio resource management DCA channels from the DCA channel list for 2.4 GHz or 5 GHz devices, use the **ap dot11** {**24ghz** | **5ghz**} **rrm channel dca remove** *number* command. To add a default DCA channel back to the DCA channel list, use the **no** form of the command.

ap dot11 [**24ghz**| **5ghz**] **rrm channel dca remove** *number*

no ap dot11 [**24ghz**| **5ghz**] **rrm channel dca remove** *number*

Syntax Description

number	Specifies the radio resource management DCA channel.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None.

This example shows how to remove default radio resource management DCA channel from the DCA list for a 2.4 GHz device, using the **ap dot11 24ghz rrm channel dca remove** command:

```
Device(config)#ap dot11 24ghz rrm channel dca remove 11
```

ap dot11 5ghz rrm channel dca chan-width-11n

To configure DCA channel width for all 802.11n radios in the 5-GHz band, enter the **ap dot11 5ghz rrm channel dca chan-width-11n** *width* command. To disable DCA channel width for all 802.11n radios in the 5-GHz band, use the **no** form of the command.

ap dot11 5ghzrrm channel dca chan-width-11n {**20**|**40**}

noap dot11 5ghzrrm channel dca chan-width-11n {**20**|**40**}

Syntax Description

chan-width-11n	Specifies DCA channel width for all 802.11n radios in the 5-GHz band.
20	Sets the channel width for 802.11n radios to 20 MHz.
40	Sets the channel width for 802.11n radios to 40 MHz.

Command Default

The default channel width is 20.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None.

This example shows how to set the channel width for the 802.11n radios to 40 MHz, using the **ap dot11 5ghz rrm channel dca chan-width-11n** command:

```
Device(config)#ap dot11 5ghz rrm channel dca chan-width-11n 40
```

ap dot11 rrm coverage

To enable 802.11 coverage hole detection, use the **ap dot11 rrm coverage** command.

ap dot11 {**24ghz**| **5ghz**} **rrm coverage** [**data** {**fail-percentage** *percentage*| **packet-count** *count*| **rssi-threshold** *threshold*}| **exceptional global** *value*| **level global** *value*| **voice** {**fail-percentage** *percentage*| **packet-count** *packet-count*| **rssi-threshold** *threshold*}]

Syntax Description

data	Specifies 802.11 coverage hole-detection data packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
packet-count *count*	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
rssi-threshold *threshold*	Specifies 802.11 minimum-receive-coverage level for voice packets.
exceptional global *value*	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global *value*	Specifies 802.11 Cisco AP client-minimum-exception level between 1 and 75 clients.
voice	Specifies 802.11 coverage Hole-Detection for voice packets.
fail-percentage *percentage*	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
packet-count *packet-count*	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold *threshold*	Specifies 802.11 minimum receive coverage level for voice packets.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you enable coverage hole-detection, the device 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 **ap dot11 {24ghz | 5ghz} rrm coverage packet-count** and **ap dot11 {24ghz | 5ghz} rrm coverage fail-percentage** commands for a 5-second period, the client is considered to be in a pre-alarm condition. The device 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

ap dot11 {24ghz | 5ghz} rrm coverage level-global and **ap dot11 {24ghz | 5ghz} rrm coverage exceptional-global** commands over a 90-second period. The device determines whether the coverage hole can be corrected and, if appropriate, mitigate the coverage hole by increasing the transmit power level for that specific access point.

This example shows how to set the RSSI-threshold for data in 5-GHz band.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm coverage data rssi-threshold -80
```

ap dot11 rrm group-member

To configure members in 802.11 static RF group, use the **ap dot11 rrm group-member** command. To remove the member, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

no ap dot11 {**24ghz**| **5ghz**} **rrm group-member** *controller-name controller-ip*

Syntax Description

controller-name	Specifies the name of the controller to be added.
controller-ip	Specifies the IP address of the controller to be added.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to add a controller in the 5-GHz automatic-RF group

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm group-member ABC 10.1.1.1
```

ap dot11 rrm monitor

To monitor the 802.11-band statistics, use the **ap dot11 rrm monitor** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm monitor** {**channel-list**| {**all**| **country**| **dca**}| **coverage**| **load**| **noise**| **signal**}

no ap dot11 {**24ghz**| **5ghz**} **rrm monitor** {**channel-list**| **coverage**| **load**| **noise**| **signal**}

Syntax Description

channel-list	Sets the 802.11 noise/interference/rogue monitoring channel-list.
all	Specifies to monitor all the channels.
country	Specifies to monitor channels used in configured country code
dca	Specifies to monitor channels used by dynamic channel assignment.
coverage	Specifies 802.11 coverage measurement interval. The range is between 60 and 3600 in seconds
load	Specifies 802.11 load measurement interval. The range is between 60 and 3600 in seconds
noise	Specifies 802.11 noise measurement interval (channel scan interval). The range is between 60 and 3600 in seconds
signal	Specifies 802.11 signal measurement interval (neighbor packet frequency). The range is between 60 and 3600 in seconds

Command Default

None.

Command Modes

Interface Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to enable monitoring all the 5-GHz band channels.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm monitor channel-list all
```

ap dot11 rrm profile

To configure Cisco lightweight access point profile settings on supported 802.11 networks, use the **ap dot11 rrm profile** command.

ap dot11 {**24ghz**| **5ghz**} **rrm profile** {**customize**| **foreign** *value*| **noise** *value*| **throughput** *value*| **utilization** *value*}

Syntax Description

customize	Enables performance profiles.
foreign *value*	Specifies the 802.11 foreign 802.11 interference threshold value. The range is between 0 and 100 percent.
noise *value*	Specifies the 802.11 foreign noise threshold value. The range is between -127 and 0 dBm
throughput *value*	Specifies the 802.11a Cisco AP throughput threshold value. The range is between 1000 and 10000000 bytes per second
utilization *value*	Specifies the 802.11a RF utilization threshold value. The range is between 0 and 100 percent

Command Default

Disabled.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to set the threshold value for the noise parameter.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm profile noise -50
```

ap dot11 rrm tpc-threshold

To configure the tx-power control threshold used by RRM for auto power assignment, use the **ap dot11 rrm tpc-threshold** command. To disable, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm tpc-threshold** *value*

no ap dot11 {**24ghz**| **5ghz**} **rrm tpc-threshold**

Syntax Description

value	Specifies the power value. The range is between -80 and -50.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to configure the tx-power control threshold used by RRM for auto power assignment.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm tpc-threshold -60
```

ap dot11 rrm txpower

To configure the 802.11 tx-power level, use the **ap dot11 rrm txpower** command. To disable the 802.11 tx-power level, use the **no** form of the command.

ap dot11 {**24ghz**| **5ghz**} **rrm txpower** {**auto**| **max** *powerLevel*| **min** *powerLevel*| **once**| *power-level*}

noap dot11 {**24ghz**| **5ghz**} **rrm txpower** {**auto**| **max** *powerLevel*| **min** *powerLevel*| **once**| *power-level*}

Syntax Description

auto	Enables auto-RF.
max *powerLevel*	Configures maximum auto-RF tx power. The range is between -10 to -30.
min *powerLevel*	Configures minimum auto-RF tx power. The range is between -10 to -30.
once	Enables one-time auto-RF.

Command Default

None.

Command Modes

Interface configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The **no** form of the command is introduced.

Usage Guidelines

None.

This example shows how to enables auto-RF once.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 5ghz rrm txpower once
```

show ap dot11 24ghz

To display the 2.4 GHz RRM parameters, use the **show ap dot11 24ghz** command.

show ap dot11 24ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

Syntax Description

ccx	Displays the 802.11b CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11b channel assignment.
coverage	Displays the configuration and statistics of the 802.11b coverage.
group	Displays the configuration and statistics of the 802.11b grouping.
l2roam	Displays 802.11b l2roam information.
logging	Displays the configuration and statistics of the 802.11b event logging.
monitor	Displays the configuration and statistics of the 802.11b monitoring.
profile	Displays 802.11b profiling information for all Cisco APs.
receiver	Displays the configuration and statistics of the 802.11b receiver.
summary	Displays the configuration and statistics of the 802.11b Cisco APs.
txpower	Displays the configuration and statistics of the 802.11b transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.
This example shows how to display configuration and statistics of the 802.11b coverage.

```
Device#show ap dot11 24ghz coverage

Coverage Hole Detection
  802.11b Coverage Hole Detection Mode            : Enabled
  802.11b Coverage Voice Packet Count             : 100 packet(s)
  802.11b Coverage Voice Packet Percentage        : 50%
  802.11b Coverage Voice RSSI Threshold           : -80 dBm
  802.11b Coverage Data Packet Count              : 50 packet(s)
  802.11b Coverage Data Packet Percentage         : 50%
  802.11b Coverage Data RSSI Threshold            : -80 dBm
  802.11b Global coverage exception level         : 25 %
  802.11b Global client minimum exception level   : 3 clients
```

show ap dot11 5ghz

To display the 5GHz RRM parameters, use the **show ap dot11 5ghz** command.

show ap dot11 5ghz {**ccx**| **channel**| **coverage**| **group**| **l2roam**| **logging**| **monitor**| **profile**| **receiver**| **summary**| **txpower**}

Syntax Description

ccx	Displays the 802.11a CCX information for all Cisco APs.
channel	Displays the configuration and statistics of the 802.11a channel assignment.
coverage	Displays the configuration and statistics of the 802.11a coverage.
group	Displays the configuration and statistics of the 802.11a grouping.
l2roam	Displays 802.11a l2roam information.
logging	Displays the configuration and statistics of the 802.11a event logging.
monitor	Displays the configuration and statistics of the 802.11a monitoring.
profile	Displays 802.11a profiling information for all Cisco APs.

receiver	Displays the configuration and statistics of the 802.11a receiver.
summary	Displays the configuration and statistics of the 802.11a Cisco APs.
txpower	Displays the configuration and statistics of the 802.11a transmit power control.

Command Default

None.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows configuration and statistics of 802.11a channel assignment.

```
Device#show ap dot11 5ghz channel

Automatic Channel Assignment
  Channel Assignment Mode                    : AUTO
  Channel Update Interval                    : 12 Hours
  Anchor time (Hour of the day)              : 20
  Channel Update Contribution                : SNI..
  Channel Assignment Leader                  : web (9.9.9.2)
  Last Run                                   : 16534 seconds ago
  DCA Sensitivity Level                      : MEDIUM (15 dB)
  DCA 802.11n Channel Width                  : 40 Mhz
  Channel Energy Levels
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  Channel Dwell Times
      Minimum                                : unknown
      Average                                : unknown
      Maximum                                : unknown
  802.11a 5 GHz Auto-RF Channel List
  Allowed Channel List                       : 36,40,44,48,52,56,60,64,149,153,1

                57,161
  Unused Channel List                        : 100,104,108,112,116,132,136,140,1

                65
  802.11a 4.9 GHz Auto-RF Channel List
  Allowed Channel List                       :
  Unused Channel List                        : 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

                15,16,17,18,19,20,21,22,23,24,25,26
  DCA Outdoor AP option                      : Disabled
```

PART XII

Security

- Security Commands, page 653

CHAPTER 13

Security Commands

- aaa accounting, page 655
- aaa accounting dot1x, page 658
- aaa accounting identity, page 659
- aaa authentication dot1x, page 661
- aaa authorization, page 662
- aaa new-model, page 666
- access-session mac-move deny, page 667
- action, page 669
- authentication host-mode, page 670
- authentication mac-move permit, page 671
- authentication priority, page 672
- authentication violation, page 675
- clear errdisable interface vlan, page 676
- clear mac address-table, page 677
- deny (MAC access-list configuration), page 678
- device-role (IPv6 snooping), page 682
- device-role (IPv6 nd inspection), page 682
- device-tracking policy, page 683
- dot1x critical (global configuration), page 685
- dot1x max-start, page 685
- dot1x test eapol-capable, page 686
- dot1x test timeout, page 687
- dot1x timeout, page 688
- epm access-control open, page 690

- ip admission, page 691
- ip admission name, page 692
- ip device tracking maximum, page 694
- ip device tracking probe, page 695
- ip dhcp snooping database, page 696
- ip dhcp snooping information option format remote-id, page 697
- ip dhcp snooping verify no-relay-agent-address, page 698
- ip http access-class, page 699
- ip source binding, page 700
- ip verify source, page 701
- ipv6 access-list, page 702
- ipv6 snooping policy, page 704
- limit address-count, page 705
- mab request format attribute 32, page 706
- match (access-map configuration), page 707
- no authentication logging verbose, page 709
- no dot1x logging verbose, page 709
- no mab logging verbose, page 710
- permit (MAC access-list configuration), page 711
- protocol (IPv6 snooping), page 714
- security level (IPv6 snooping), page 715
- security passthru, page 716
- show aaa clients, page 717
- show aaa command handler, page 717
- show aaa local, page 718
- show aaa servers, page 719
- show aaa sessions, page 720
- show authentication history, page 721
- show authentication sessions, page 721
- show dot1x, page 724
- show eap pac peer, page 725
- show ip dhcp snooping statistics, page 725
- show radius server-group, page 728

- show storm-control, page 729
- show vlan access-map, page 731
- show vlan filter, page 732
- show vlan group, page 732
- storm-control, page 733
- switchport port-security aging, page 736
- switchport port-security mac-address, page 737
- switchport port-security maximum, page 739
- switchport port-security violation, page 741
- tracking (IPv6 snooping), page 742
- trusted-port, page 744
- wireless dot11-padding, page 745
- wireless security dot1x, page 745
- wireless security lsc, page 747
- wireless security strong-password, page 748
- wireless wps ap-authentication, page 749
- wireless wps auto-immune, page 750
- wireless wps cids-sensor, page 750
- wireless wps client-exclusion, page 751
- wireless wps mfp infrastructure, page 752
- wireless wps rogue, page 753
- wireless wps shun-list re-sync, page 754
- vlan access-map, page 754
- vlan filter, page 756
- vlan group, page 757

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

aaa accouting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

no aaa accouting {**auth-proxy** | **system** | **network** | **exec** | **connections** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests.
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the **autocommand** command.
connection	Provides information about all outbound connections made from the network access server.
commands *level*	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
list-name	Character string used to name the list of at least one of the accounting methods decribed in
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	Sends a "stop" accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
group groupname	At least one of the keywords described in Table 23: AAA accounting Methods, on page 657

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 23: AAA accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.

In Table 23: AAA accounting Methods, on page 657, the **group radius** and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- RADIUS—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- TACACS+—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method* , where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.

Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting

notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The none keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix RADIUS Attributes in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix TACACS+ Attribute-Value Pairs in the *Cisco IOS Security Configuration Guide.*

Note This command cannot be used with TACACS or extended TACACS.

This example defines a default commands accounting menthod list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
```

This example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The aaa accounting commands activates authentication proxy accouting.

```
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
```

aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x**command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

aaa accounting dot1x {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting dot1x {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Specifies the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.

broadcast	Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* — Name of a server group. • **radius** — Lists of all RADIUS hosts. • **tacacs+** — Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS accounting.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) accounting for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

aaa accounting identity {*name* | **default** } **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ...] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**}...]}

no aaa accounting identity {*name* | **default** }

Syntax Description

name	Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: • *name* — Name of a server group. • **radius** — Lists of all RADIUS hosts. • **tacacs+** — Lists of all TACACS+ hosts. The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.
radius	(Optional) Enables RADIUS authorization.
tacacs+	(Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To enable AAA accounting identity, you need to enable policy mode. To enable policy mode, enter the **authentication display new-style** command in privileged EXEC mode.

This example shows how to configure IEEE 802.1x accounting identity:

```
Device# authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
    to NVRAM in NEW-style config, and if you subsequently
    reload the router without reverting to legacy config and
    saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
    will only become IPv6-capable once you have entered new-
    style config manually, or have reloaded with config saved
    in 'authentication display new' mode.

Device# configure terminal
Device(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode on the switch stack or on a standalone switch. To disable authentication, use the **no** form of this command.

aaa authentication dot1x {**default**} *method1*

no aaa authentication dot1x {**default**} *method1*

Syntax Description

default	The default method when a user logs in. Use the listed authentication method that follows this argument.
method1	Specifies the server authentication. Enter the **group radius** keywords to use the list of all RADIUS servers for authentication. **Note** Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

Command Default

No authentication is performed.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name* } [*method1* [*method2* ...]]

no aaa authorization { **auth-proxy** | **cache** | **commands** *level* | **config-commands** | **configuration** | **console** | **credential-download** | **exec** | **multicast** | **network** | **reverse-access** |**template**} {**default** | *list_name* } [*method1* [*method2* ...]]

Syntax Description

auth-proxy	Runs authorization for authentication proxy services.
cache	Configures the authentication, authorization, and accounting (AAA) server.
commands	Runs authorization for all commands at the specified privilege level.
level	Specific command level that should be authorized. Valid entries are 0 through 15.
config-commands	Runs authorization to determine whether commands entered in configuration mode are authorized.
configuration	Downloads the configuration from the AAA server.
console	Enables the console authorization for the AAA server.
credential-download	Downloads EAP credential from Local/RADIUS/LDAP.
exec	Enables the console authorization for the AAA server.

multicast	Downloads the multicast configuration from the AAA server.
network	Runs authorization for all network-related service requests, including Serial Line Internet Protocol (SLIP), PPP, PPP Network Control Programs (NCPs), and AppleTalk Remote Access (ARA).
reverse-access	Runs authorization for reverse access connections, such as reverse Telnet.
template	Enables template authorization for the AAA server.
default	Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.
list_name	Character string used to name the list of authorization methods.
method1 [*method2...*]	(Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.

Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.

Note In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius-server host** and **tacacs-server host** commands to configure the host servers. Use the **aaa group server radius**, **aaa group server ldap**, and **aaa group server tacacs+** commands to create a named group of servers.

This table describes the method keywords.

Table 24: aaa authorization Methods

Keyword	Description
cache *group-name*	Uses a cache server group for authorization.
group *group-name*	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the **server group** *group-name* command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the **aaa group server radius** command.
grouptacacs+	Uses the list of all TACACS+ servers for authentication as defined by the **aaa group server tacacs+** command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. **Note** The **if-authenticated** method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups — The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated — The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local— The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None — The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS —The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+ — The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- Commands — Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC — Applies to the attributes associated with a user EXEC terminal session.
- Network — Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.

Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- Reverse Access — Applies to reverse Telnet sessions.
- Configuration — Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.

Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

The following example shows how to define the network authorization method list named mygroup, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Device(config)#  aaa authorization network mygroup group radius local
```

aaa new-model

To enable the authentication, authorization, and accounting (AAA) access control model, issue the **aaa new-model** command in global configuration mode. To disable the AAA access control model, use the **no** form of this command.

aaa new-model

no aaa new-model

Syntax Description

This command has no arguments or keywords.

Command Default

AAA is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2SE	This command was implemented on Cisco Catalyst 3850 Series Switches.

Usage Guidelines

This command enables the AAA access control system.

If the **login local** command is configured for a virtual terminal line (VTY), and the **aaa new-model** command is removed, you must reload the switch to get the default configuration or the **login** command. If the switch is not reloaded, the switch defaults to the **login local** command under the VTY.

Note We do not recommend removing the **aaa new-model** command.

The following example shows this restriction:

```
Switch(config)# aaa new-model
Switch(config)# line vty 0 15
Switch(config-line)# login local
Switch(config-line)# exit
Switch(config)# no aaa new-model
Switch(config)# exit
Switch# show running-config | b line vty

line vty 0 4
 login local  !<=== Login local instead of "login"
line vty 5 15
 login local
!
```

The following example initializes AAA:

```
Switch(config)# aaa new-model
Switch(config)#
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication arap	Enables an AAA authentication method for ARAP using TACACS+.
aaa authentication enable default	Enables AAA authentication to determine if a user can access the privileged command level.
aaa authentication login	Sets AAA authentication at login.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.

access-session mac-move deny

To disable MAC move on a device, use the **access-session mac-move deny** global configuration command. To return to the default setting, use the **no** form of this command.

access-session mac-move deny

no access-session mac-move deny

Syntax Description

This command has no arguments or keywords.

Command Default

MAC move is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no** form of this command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# no access-session mac-move deny
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.

Command	Description
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
show authentication	Displays information about authentication manager events on the switch.

action

To set the action for the VLAN access map entry, use the **action** command in access-map configuration mode. To return to the default setting, use the **no** form of this command.

action {**drop**| **forward**}

no action

Syntax Description

drop	Drops the packet when the specified conditions are matched.
forward	Forwards the packet when the specified conditions are matched.

Command Default

The default action is to forward packets.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access-map configuration mode, use the **match access-map** configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

This example shows how to identify and apply a VLAN access map (vmap4) to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode {**multi-auth** | **multi-domain** | **multi-host** | **single-host**}

no authentication host-mode

Syntax Description

multi-auth	Enables multiple-authorization mode (multi-auth mode) on the port.
multi-domain	Enables multiple-domain mode on the port.
multi-host	Enables multiple-host mode on the port.
single-host	Enables single-host mode on the port.

Command Default

Single host mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

This example shows how to enable multi-auth mode on a port:

```
Device(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Device(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Device(config-if)# authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Device(config-if)# authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface** *interface* **details** privileged EXEC command.

authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

authentication mac-move permit

no authentication mac-move permit

Syntax Description

This command has no arguments or keywords.

Command Default

MAC move is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This is a legacy command. The new command is **access-session mac-move deny**.

The command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# authentication mac-move permit
```

Related Commands

Command	Description
access-session mac-move deny	Disables MAC move on a device.
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enable or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
show authentication	Displays information about authentication manager events on the switch.

authentication priority

To add an authentication method to the port-priority list, use the **authentication priority** command in interface configuration mode. To return to the default, use the **no** form of this command.

authentication priority [**dot1x** | **mab**] {**webauth**}

no authentication priority [**dot1x** | **mab**] {**webauth**}

Syntax Description

dot1x	(Optional) Adds 802.1x to the order of authentication methods.
mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
webauth	Adds web authentication to the order of authentication methods.

Command Default

The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.

Note If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the **dot1x**, **mab**, and **webauth** keywords to change this default order.

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority dotx webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority mab webauth
```

Related Commands

Command	Description
authentication control-direction	Configures the port mode as unidirectional or bidirectional.
authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
authentication fallback	Enables a web authentication fallback method.
authentication host-mode	Allows hosts to gain access to a controlled port.
authentication open	Enables open access on a port.
authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
authentication periodic	Enables automatic reauthentication on a port.
authentication port-control	Configures the authorization state of a controlled port.
authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.
authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
authentication violation	Specifies the action to be taken when a security violation occurs on a port.
mab	Enables MAC authentication bypass on a port.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about current Auth Manager sessions.

Command	Description
show authentication sessions interface	Displays information about the Auth Manager for a given interface.

authentication violation

To configure the violation modes that occur when a new device connects to a port or when a new device connects to a port after the maximum number of devices are connected to that port, use the **authentication violation** command in interface configuration mode.

authentication violation { **protect**|**replace**|**restrict**|**shutdown** }

no authentication violation { **protect**|**replace**|**restrict**|**shutdown** }

Syntax Description

protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
replace	Removes the current session and initiates authentication with the new host.
restrict	Generates a syslog error when a violation error occurs.
shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

Command Default

Authentication violation shutdown mode is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device(config-if)# authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Device(config-if)# authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Device(config-if)# authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Device(config-if)# authentication violation replace
```

You can verify your settings by entering the **show authentication** privileged EXEC command.

clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

clear errdisable interface *interface-id* **vlan** [*vlan-list*]

Syntax Description

interface-id	Specifies an interface.
vlan list	(Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can reenable a port by using the **shutdown** and **no shutdown** interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable** interface command.

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands

Command	Description
errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
errdisable recovery	Configures the recovery mechanism variables.
show errdisable detect	Displays error-disabled detection status.
show errdisable recovery	Displays error-disabled recovery timer information.
show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

clear mac address-table {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **move update** | **notification**}

Syntax Description

dynamic	Deletes all dynamic MAC addresses.
address *mac-addr*	(Optional) Deletes the specified dynamic MAC address.
interface *interface-id*	(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan *vlan-id*	(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.
move update	Clears the MAC address table move-update counters.
notification	Clears the notifications in the history table and reset the counters.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

This example shows how to remove a specific MAC address from the dynamic address table:

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands

Command	Description
mac address-table notification	Enables the MAC address notification feature.
mac address-table move update {**receive** | **transmit**}	Configures MAC address-table move update on the switch.
show mac address-table	Displays the MAC address table static and dynamic entries.
show mac address-table move update	Displays the MAC address-table move update information on the switch.
show mac address-table notification	Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended.
snmp trap mac-notification change	Enables the SNMP MAC address notification trap on a specific interface.

deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the **deny** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a deny condition from the named MAC access list, use the **no** form of this command.

deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

no deny {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042**

| **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos** *cos*]

Syntax Description

any	Denies any source or destination MAC address.
host *src-MAC-addr* | *src-MAC-addr mask*	Defines a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Defines a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. The type is 0 to 65535, specified in hexadecimal. The mask is a mask of don't care bits applied to the EtherType before testing for a match.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.

lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.
mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.
cos *cos*	(Optional) Specifies a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the **cos** option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

Mac-access list configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the table.

Table 25: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novel Name**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Device(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.
show access-lists	Displays access control lists configured on a switch.

device-role (IPv6 snooping)

To specify the role of the device attached to the port, use the **device-role** command in IPv6 snooping configuration mode.

device-role {**node** | **switch**}

Syntax Description

node	Sets the role of the attached device to node.
switch	Sets the role of the attached device to switch.

Command Default

The device role is node.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is node.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
```

device-role (IPv6 nd inspection)

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode.

device-role {**host** | **monitor** | **router** | **switch**}

Syntax Description

host	Sets the role of the attached device to host.
monitor	Sets the role of the attached device to monitor.
router	Sets the role of the attached device to router.
switch	Sets the role of the attached device to switch.

Command Default

The device role is host.

Command Modes

ND inspection policy configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the monitor keyword does not allow inbound RA or redirect messages. When the monitor keyword is used, devices that need these messages will receive them.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level. The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)#  ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

device -tracking policy *policy-name*

no device-tracking policy *policy-name*

Syntax Description

policy-name	User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

A device tracking policy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Use the SISF-based **device-tracking policy** command to create a device tracking policy. When the **device-tracking policy** command is enabled, the configuration mode changes to device-tracking configuration mode. In this mode, the administrator can configure the following first-hop security commands:

- (Optional) **device-role**{**node**] | **switch**}—Specifies the role of the device attached to the port. Default is **node**.
- (Optional) **limit address-count** *value*—Limits the number of addresses allowed per target.
- (Optional) **no**—Negates a command or sets it to defaults.
- (Optional) **destination-glean**{**recovery**| **log-only**}[**dhcp**]}—Enables binding table recovery by data traffic source address gleaning.
- (Optional) **data-glean**{**recovery**| **log-only**}[**dhcp** | **ndp**]}—Enables binding table recovery using source or data address gleaning.
- (Optional) **security-level**{**glean**|**guard**|**inspect**}—Specifies the level of security enforced by the feature. Default is **guard.**

  glean—Gleans addresses from messages and populates the binding table without any verification.

  guard—Gleans addresses and inspects messages. In addition, it rejects RA and DHCP server messages. This is the default option.

  inspect—Gleans addresses, validates messages for consistency and conformance, and enforces address ownership.

- (Optional) **tracking** {**disable** | **enable**}—Specifies a tracking option.
- (Optional) **trusted-port**—Sets up a trusted port. It disables the guard on applicable targets. Bindings learned through a trusted port have preference over bindings learned through any other port. A trusted port is given preference in case of a collision while making an entry in the table.

This example shows how to configure an a device-tracking policy:

```
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
```

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical eapol

Syntax Description

eapol	Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.

Command Default

eapol is disabled

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Device(config)# dot1x critical eapol
```

dot1x max-start

To set the maximum number of Extensible Authentication Protocol over LAN (EAPOL) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description

number	Maximum number of times that the router sends an EAPOL start frame. The value is from 1 to 10. The default is 3.

Command Default

The default maximum number setting is 3.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enter the **switchport mode access** interface configuration command on a switch port before entering this command.

The following example shows that the maximum number of EAPOL Start requests has been set to 5:

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x max-start 5
```

dot1x test eapol-capable

To monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x, use the **dot1x test eapol-capable** command in privileged EXEC mode on the switch stack or on a standalone switch.

dot1x test eapol-capable [**interface** *interface-id*]

Syntax Description

interface *interface-id*	(Optional) Port to be queried.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

Related Commands

Command	Description
dot1x test timeout *timeout*	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode on the switch stack or on a standalone switch.

dot1x test timeout *timeout*

Syntax Description

timeout	Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds.

Command Default

The default setting is 10 seconds.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure the timeout used to wait for EAPOL response.

There is not a no form of this command.

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

Related Commands

Command	Description
dot1x test eapol-capable [**interface** *interface-id*]	Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts, use the **no** form of this command.

dot1x timeout {**auth-period** *seconds* | **held-period** *seconds* | **quiet-period** *seconds* | **ratelimit-period** *seconds* | **server-timeout** *seconds* | **start-period** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

Syntax Description

auth-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30.
held-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 60
quiet-period *seconds*	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The range is from 1 to 65535. The default is 60

ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
server-timeout *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The range is from 1 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30.
supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. The range is from 1 to 65535. The default is 30.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • The range is from 1 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default

Periodic reauthentication and periodic rate-limiting are done.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

epm access-control open

no epm access-control open

Syntax Description

This command has no arguments or keywords.

Command Default

The default directive applies.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

You can verify your settings by entering the **show running-config** privileged EXEC command.

This example shows how to configure an open directive.

```
Device(config)# epm access-control open
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

ip admission

To enable web authentication, use the **ip admission** command in interface configuration mode. You can also use this command in fallback-profile configuration mode. To disable web authentication, use the **no** form of this command.

ip admission *rule*

no ip admission *rule*

Syntax Description

rule	IP admission rule name.

Command Default

Web authentication is disabled.

Command Modes

Interface configuration

Fallback-profile configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **ip admission** command applies a web authentication rule to a switch port.

This example shows how to apply a web authentication rule to a switchport:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

no ip admission name *name* {**consent** | **proxy http**} [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** {*acl* | *acl-name*} | **service-policy type tag** *service-policy-name*]

Syntax Description

name	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the *admission-name* argument.
proxy http	Configures web authentication custom page.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199, or from 1300 through 2699 for expanded range.
acl-name	Applies a named access list to a named admission control rule.
service-policy type tag	(Optional) A control plane service policy is to be configured.

service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag***policyname* command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

Command Default

Web authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **ip admission name** command globally enables web authentication on a switch.

After you enable web authentication on a switch, use the **ip access-group in** and **ip admission web-rule** interface configuration commands to enable web authentication on a specific interface.

This example shows how to configure only web authentication on a switch port:

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.

Command	Description
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface *interface* **detail**	Displays information about the web authentication session status.
show ip admission	Displays information about NAC cached entries or the NAC configuration.

ip device tracking maximum

To configure IP device tracking parameters on a Layer 2 access port, use the **ip device tracking maximum** command in interface configuration mode. To remove the maximum value, use the **no** form of the command.

ip device tracking maximum *number*

no ip device tracking maximum

Syntax Description

number	Number of bindings created in the IP device tracking table for a port. The range is 0 (disabled) to 65535.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To remove the maximum value, use the **no ip device tracking maximum** command.

To disable IP device tracking, use the **ip device tracking maximum 0** command.

This example shows how to configure IP device tracking parameters on a Layer 2 access port:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

no ip device tracking probe {**count** *number*| **delay** *seconds*| **interval** *seconds*| **use-svi** *address*}

Syntax Description

count *number*	Sets the number of times that the device sends the ARP probe. The range is from 1 to 255.
delay *seconds*	Sets the number of seconds that the device waits before sending the ARP probe. The range is from 1 to 120.
interval *seconds*	Sets the number of seconds that the device waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
use-svi	Uses the switch virtual interface (SVI) IP address as source of ARP probes.

Command Default

The count number is 3.

There is no delay.

The interval is 30 seconds.

The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **use-svi** keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

This example shows how to set SVI as the source for ARP probes:

```
Device(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

ip dhcp snooping database {**crashinfo:***url* | **flash:***url* | **ftp:***url* | **http:***url* | **https:***url* | **rcp:***url* | **scp:***url* | **tftp:***url* | **timeout** *seconds* | **usbflash0:***url* | **write-delay** *seconds*}

no ip dhcp snooping database [**timeout** | **write-delay**]

Syntax Description

crashinfo:*url*	Specifies the database URL for storing entries using crashinfo.
flash:*url*	Specifies the database URL for storing entries using flash.
ftp:*url*	Specifies the database URL for storing entries using FTP.
http:*url*	Specifies the database URL for storing entries using HTTP.
https:*url*	Specifies the database URL for storing entries using secure HTTP (https).
rcp:*url*	Specifies the database URL for storing entries using remote copy (rcp).
scp:*url*	Specifies the database URL for storing entries using Secure Copy (SCP).
tftp:*url*	Specifies the database URL for storing entries using TFTP.
timeout *seconds*	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
usbflash0:*url*	Specifies the database URL for storing entries using USB flash.

write-delay *seconds*	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default

The DHCP-snooping database is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device(config)#  ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Device(config)#  ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the switch to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

no ip dhcp snooping information option format remote-id {**hostname** | **string** *string*}

Syntax Description

hostname	Specify the switch hostname as the remote ID.
string *string*	Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

Command Default

The switch MAC address is the remote ID.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.

Note If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.

This example shows how to configure the option- 82 remote-ID suboption:

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```

ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

ip dhcp snooping verify no-relay-agent-address

no ip dhcp snooping verify no-relay-agent-address

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenable verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.

ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

no ip http access-class { *access-list-number* | **ipv4** { *access-list-number* | *access-list-name* } | **ipv6** *access-list-name* }

Syntax Description

ipv4	Specifies the IPv4 access list to restrict access to the secure HTTP server.
ipv6	Specifies the IPv6 access list to restrict access to the secure HTTP server.
access-list-number	Standard IP access list number in the range 0 to 99, as configured by the **access-list** global configuration command.
access-list-name	Name of a standard IPv4 access list, as configured by the **ip access-list** command.

Command Default

No access list is applied to the HTTP server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified. The **ipv4** and **ipv6** keyword were added.
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
```

The following example shows how to define an IPv4 named access list as and assign it to the HTTP server.

```
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
Device(config)# ip http access-class ipv4 Internet_filter
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip source binding

To add a static IP source binding entry, use the **ip source binding** command. Use the **no** form of this command to delete a static IP source binding entry

ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

no ip source binding *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

Syntax Description

mac-address	Binding MAC address.
vlan *vlan-id*	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
ip-address	Binding IP address.
interface *interface-id*	ID of the physical interface.

Command Default

No IP source bindings are configured.

Command Modes

Global configuration.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can use this command to add a static IP source binding entry only.

The **no** format deletes the corresponding IP source binding entry. It requires the exact match of all required parameter in order for the deletion to be successful. Note that each static IP binding entry is keyed by a MAC address and a VLAN number. If the command contains the existing MAC address and VLAN number, the existing binding entry is updated with the new parameters instead of creating a separate binding entry.

This example shows how to add a static IP source binding entry:

```
Device# configure terminal
Deviceconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

ip verify source [**mac-check**][**tracking**]

no ip verify source

Syntax Description

mac-check	(Optional) Enables IP source guard with MAC address verification.
tracking	(Optional) Enables IP port security to learn static IP address learning on a port.

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP address filtering and MAC address verification, use the **ip verify source mac-check** interface configuration command.

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

This example shows how to enable IP source guard with MAC address verification:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*

noipv6 access-list *access-list-name* | **client** *permit-control-packets*| **log-update** *threshold* | **role-based** *list-name*

Syntax Description

ipv6 *access-list-name*	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode. *access-list-name* - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold *threshold-in-msgs*	Determines how syslog messages are generated after the initial packet match. *threshold-in-msgs*- Number of packets generated.
role-based *list-name*	Creates a role-based IPv6 ACL.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification

Usage Guidelines

IPv6 ACLs are defined by using the **ipv6 access-list**command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit**commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list**command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.

Note IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes

use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6 snooping policy

Note All existing IPv6 Snooping commands (prior to Cisco IOS XE Denali 16.1.1) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, seedevice-tracking policy

To configure an IPv6 snooping policy and enter IPv6 snooping configuration mode, use the **ipv6 snooping policy** command in global configuration mode. To delete an IPv6 snooping policy, use the **no** form of this command.

ipv6 snooping policy *snooping-policy*

no ipv6 snooping policy *snooping-policy*

Syntax Description

snooping-policy	User-defined name of the snooping policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

Command Default

An IPv6 snooping policy is not configured.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping policy** command to create an IPv6 snooping policy. When the **ipv6 snooping policy** command is enabled, the configuration mode changes to IPv6 snooping configuration mode. In this mode, the administrator can configure the following IPv6 first-hop security commands:

- The **device-role** command specifies the role of the device attached to the port.
- The **limit address-count** *maximum* command limits the number of IPv6 addresses allowed to be used on the port.
- The **protocol** command specifies that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP).
- The **security-level** command specifies the level of security enforced.
- The **tracking** command overrides the default tracking policy on a port.
- The **trusted-port** command configures a port to become a trusted port; that is, limited or no verification is performed when messages are received.

This example shows how to configure an IPv6 snooping policy:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the **no** form of this command.

limit address-count *maximum*

no limit address-count

Syntax Description

maximum	The number of addresses allowed on the port. The range is from 1 to 10000.

Command Default

The default is no limit.

Command Modes

ND inspection policy configuration

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size. The range is from 1 to 10000.
This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

mab request format attribute 32 vlan access-vlan

no mab request format attribute 32 vlan access-vlan

Syntax Description

This command has no arguments or keywords.

Command Default

VLAN-ID based MAC authentication is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands

Command	Description
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enables or disables reauthentication on a port.
authentication port-control	Enables manual control of the port authorization state.
authentication priority	Adds an authentication method to the port-priority list.
authentication timer	Configures the timeout and reauthentication parameters for an 802.1x-enabled port.
authentication violation	Configures the violation modes that occur when a new device connects to a port or when a new device connects to a port with the maximum number of devices already connected to that port.
mab	Enables MAC-based authentication on a port.
mab eap	Configures a port to use the Extensible Authentication Protocol (EAP).
show authentication	Displays information about authentication manager events on the switch.

match (access-map configuration)

To set the VLAN map to match packets against one or more access lists, use the **match** command in access-map configuration mode on the switch stack or on a standalone switch. To remove the match parameters, use the **no** form of this command.

match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

no match {**ip address** {*name*| *number*} [*name*| *number*] [*name*| *number*]...| **mac address** {*name*} [*name*] [*name*]...}

Syntax Description

ip address	Sets the access map to match packets against an IP address access list.
mac address	Sets the access map to match packets against a MAC address access list.
name	Name of the access list to match packets against.
number	Number of the access list to match packets against. This option is not valid for MAC access lists.

Command Default

The default action is to have no match parameters applied to a VLAN map.

Command Modes

Access-map configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

This example shows how to define and apply a VLAN access map vmap4 to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list al2:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

no authentication logging verbose

To filter detailed information from authentication system messages, use the **no authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no authentication logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

To filter verbose authentication system messages:

```
Device(config)# no authentication logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **no dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no dot1x logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

To filter verbose 802.1x system messages:

```
Device(config)# no dot1x logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **no mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no mab logging verbose

Syntax Description

This command has no arguments or keywords.

Command Default

All details are displayed in the system messages.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device(config)# no mab logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
no authentication logging verbose	Filters details from authentication system messages.
no dot1x logging verbose	Filters details from 802.1x system messages.
no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

{**permit** {**any** | **host***src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host***dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap***lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

nopermit {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **appletalk** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**][**cos***cos*]

Syntax Description

any	Denies any source or destination MAC address.

host *src-MAC-addr* | *src-MAC-addr mask*	Specifies a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied.
host *dst-MAC-addr* | *dst-MAC-addr mask*	Specifies a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied.
type mask	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. • *type* is 0 to 65535, specified in hexadecimal. • *mask* is a mask of don't care bits applied to the EtherType before testing for a match.
aarp	(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.
amber	(Optional) Specifies EtherType DEC-Amber.
appletalk	(Optional) Specifies EtherType AppleTalk/EtherTalk.
dec-spanning	(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.
decnet-iv	(Optional) Specifies EtherType DECnet Phase IV protocol.
diagnostic	(Optional) Specifies EtherType DEC-Diagnostic.
dsm	(Optional) Specifies EtherType DEC-DSM.
etype-6000	(Optional) Specifies EtherType 0x6000.
etype-8042	(Optional) Specifies EtherType 0x8042.
lat	(Optional) Specifies EtherType DEC-LAT.
lavc-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap *lsap-number mask*	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The *mask* is a mask of don't care bits applied to the LSAP number before testing for a match.
mop-console	(Optional) Specifies EtherType DEC-MOP Remote Console.
mop-dump	(Optional) Specifies EtherType DEC-MOP Dump.
msdos	(Optional) Specifies EtherType DEC-MSDOS.

mumps	(Optional) Specifies EtherType DEC-MUMPS.
netbios	(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).
vines-echo	(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.
vines-ip	(Optional) Specifies EtherType VINES IP.
xns-idp	(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.
cos *cos*	(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the **cos** option is configured.

Command Default

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

Command Modes

Mac-access list configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in the following table.

Table 26: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	**Novell Name**	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Device(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
show access-lists	Displays access control lists configured on a switch.

protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

protocol {**dhcp** | **ndp**}

no protocol {**dhcp** | **ndp**}

Syntax Description

dhcp	Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.
ndp	Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

Command Default

Snooping and recovery are attempted using both DHCP and NDP.

Command Modes

IPv6 snooping configuration mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol** {**dhcp** | **ndp**} command indicates that a protocol will not be used for snooping or gleaning.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```

security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

security level {**glean** | **guard** | **inspect**}

Syntax Description

glean	Extracts addresses from the messages and installs them into the binding table without performing any verification.
guard	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
inspect	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.

Command Default

The default security level is guard.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

security passthru

To modify the IPsec pass-through, use the **security passthru** command. To disable, use the no form of the command.

security passthru *ip-address*

no security passthru

Syntax Description

ip-address	IP address of the IPsec gateway (router) that is terminating the VPN tunnel.

Command Default

None.

Command Modes

wlan

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to modify IPSec pass-through.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#security passthrough 10.1.1.1
```

show aaa clients

To show AAA client statistics, use the **show aaa clients** command.

show aaa clients [**detailed**]

Syntax Description

detailed	(Optional) Shows detailed AAA client statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa clients** command:

```
Device# show aaa clients

Dropped request packets: 0
```

show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

show aaa command handler

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
    account-logon: 0, account-logoff: 0
    account-query: 0, pod: 0
    service-logon: 0, service-logoff: 0
    user-profile-push: 0, session-state-log: 0
    reauthenticate: 0, bounce-host-port: 0
    disable-host-port: 0, update-rbacl: 0
    update-sgt: 0, update-cts-policies: 0
    invalid commands: 0
    async message not sent: 0
```

show aaa local

To show AAA local method options, use the **show aaa local** command.

show aaa local {**netuser** {*name* | **all** } | **statistics** | **user lockout**}

Syntax Description

netuser	Specifies the AAA local network or guest user database.
name	Network user name.
all	Specifies the network and guest user information.
statistics	Displays statistics for local authentication.
user lockout	Specifies the AAA local locked-out user.

Command Modes User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa local statistics** command:

```
Device# show aaa local statistics

Local EAP statistics

EAP Method         Success       Fail
-------------------------------------
Unknown                  0          0
EAP-MD5                  0          0
EAP-GTC                  0          0
LEAP                     0          0
PEAP                     0          0
EAP-TLS                  0          0
EAP-MSCHAPV2             0          0
EAP-FAST                 0          0

Requests received from AAA:                 0
Responses returned from EAP:                0
Requests dropped (no EAP AVP):              0
Requests dropped (other reasons):           0
Authentication timeouts from EAP:           0

Credential request statistics
Requests sent to backend:                   0
Requests failed (unable to send):           0
Authorization results received

  Success:                                  0
  Fail:                                     0
```

show aaa servers

To shows all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

show aaa servers [**private**|**public**|[**detailed**]]

Syntax Description

detailed	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
public	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
detailed	(Optional) Displays detailed AAA server statistics.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa servers** command:

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

show aaa sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa sessions** command:

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
   Unique Id: 4025
   User Name: *not available*
   IP Address: 0.0.0.0
   Idle Time: 0
   CT Call Handle: 0
```

show authentication history

To display the authenticated sessions alive on the device, use the **show authentication history** command.

show authentication history [**min-uptime** *seconds*]

Syntax Description

min-uptime *seconds*	(Optional) Displays sessions within the minimum uptime. The range is from 1 through 4294967295 seconds.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show authentication history** command to display the authenticated sessions alive on the device.

This is an example of output from the **show authentication history** command:

```
Device# show authentication history
Interface  MAC Address     Method  Domain  Status  Uptime
Gi3/0/2    0021.d864.07c0  dot1x   DATA    Auth    38s

Session count = 1
```

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

show authentication sessions [**database**][**handle** *handle-id* [**details**]][**interface** *type number* [**details**][**mac** *mac-address* [**interface** *type number*][**method** *method-name* [**interface** *type number* [**details**] [**session-id** *session-id* [**details**]]

Syntax Description

database	(Optional) Shows only data stored in session database.
handle *handle-id*	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
details	(Optional) Shows detailed information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (**dot1x**, **mab**, or **webauth**), you may also specify an interface.
session-id *session-id*	(Optional) Specifies the particular session for which Auth Manager information is to be displayed.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

This table shows the possible operating states for the reported authentication sessions.

Table 27: Authentication Method States

State	Description
Not run	The method has not run for this session.
Running	The method is running for this session.
Failed over	The method has failed and the next method is expected to provide a result.
Success	The method has provided a successful authentication result for the session.

State	Description
Authc Failed	The method has provided a failed authentication result for the session.

This table shows the possible authentication methods.

Table 28: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions
Interface    MAC Address     Method   Domain   Status         Session ID
Gi1/0/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/0/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/0/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47
            Interface:  GigabitEthernet2/0/47
          MAC Address:  Unknown
           IP Address:  Unknown
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Guest Vlan
          Vlan Policy:  20
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000000002763C
      Acct Session ID:  0x00000002
               Handle:  0x25000000
Runnable methods list:
       Method   State
       mab      Failed over
       dot1x    Failed over
----------------------------------------
            Interface:  GigabitEthernet2/0/47
          MAC Address:  0005.5e7c.da05
           IP Address:  Unknown
            User-Name:  00055e7cda05
               Status:  Authz Success
               Domain:  VOICE
       Oper host mode:  multi-domain
     Oper control dir:  both
        Authorized By:  Authentication Server
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A3462C8000000010002A238
      Acct Session ID:  0x00000003
```

```
              Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port, use the **show dot1x** command in user EXEC mode.

show dot1x [**all** [**count** | **details** | **statistics** | **summary**]] [**interface** *type number* [**details** | **statistics**]] [**statistics**]

Syntax Description

all	(Optional) Displays the IEEE 802.1x information for all interfaces.
count	(Optional) Displays total number of authorized and unauthorized clients.
details	(Optional) Displays the IEEE 802.1x interface details.
statistics	(Optional) Displays the IEEE 802.1x statistics for all interfaces.
summary	(Optional) Displays the IEEE 802.1x summary for all interfaces.
interface *type number*	(Optional) Displays the IEEE 802.1x status for the specified port.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show dot1x all** command:

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version            3
```

This is an example of output from the **show dot1x all count** command:

```
Device# show dot1x all count
Number of Dot1x sessions
------------------------------
Authorized Clients        = 0
UnAuthorized Clients      = 0
Total No of Client        = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Device# show dot1x statistics
Dot1x Global Statistics for
---------------------------------------------
RxStart = 0     RxLogoff = 0    RxResp = 0      RxRespID = 0
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 0

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 0     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

show eap pac peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Device> show eap pac peers
No PACs stored
```

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC mode.

show ip dhcp snooping statistics [**detail**]

Syntax Description

detail	(Optional) Displays detailed statistics information.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Device> show ip dhcp snooping statistics

 Packets Forwarded                                    = 0
 Packets Dropped                                      = 0
 Packets Dropped From untrusted ports                 = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Device> show ip dhcp snooping statistics detail

 Packets Processed by DHCP Snooping                   = 0
 Packets Dropped Because
   IDB not known                                      = 0
   Queue full                                         = 0
   Interface is in errdisabled                        = 0
   Rate limit exceeded                                = 0
   Received on untrusted ports                        = 0
   Nonzero giaddr                                     = 0
   Source mac not equal to chaddr                     = 0
   Binding mismatch                                   = 0
   Insertion of opt82 fail                            = 0
   Interface Down                                     = 0
   Unknown output interface                           = 0
   Reply output port equal to input port              = 0
   Packet denied by platform                          = 0
```

This table shows the DHCP snooping statistics and their descriptions:

Table 29: DHCP Snooping Statistics

DHCP Snooping Statistic	Description
Packets Processed by DHCP Snooping	Total number of packets handled by DHCP snooping, including forwarded and dropped packets.

DHCP Snooping Statistic	Description
Packets Dropped Because IDB not known	Number of errors when the input interface of the packet cannot be determined.
Queue full	Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports.
Interface is in errdisabled	Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed.
Rate limit exceeded	Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.
Received on untrusted ports	Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.
Nonzero giaddr	Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **no ip dhcp snooping information option allow-untrusted** global configuration command is not configured and a packet received on an untrusted port contained option-82 data.
Source mac not equal to chaddr	Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the **ip dhcp snooping verify mac-address** global configuration command is configured.
Binding mismatch	Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header.
Insertion of opt82 fail	Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet.
Interface Down	Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response.

DHCP Snooping Statistic	Description
Unknown output interface	Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped.
Reply output port equal to input port	Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports.
Packet denied by platform	Number of times the packet has been denied by a platform-specific registry.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command.

show radius server-group {*name* | **all**}

Syntax Description

name	Name of the server group. The character string used to name the group of servers must be defined using **the aaa group server radius** command.
all	Displays properties for all of the server groups.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

This is an example of output from the **show radius server-group all** command:

```
Device# show radius server-group all
```

```
Server group radius
    Sharecount = 1  sg_unconfigured = FALSE
    Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

Table 30: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either standard or nonstandard. The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

show storm-control

To display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history, use the **show storm-control** command in user EXEC mode.

show storm-control [*interface-id*] [**broadcast**| **multicast**| **unicast**]

Syntax Description

interface-id	(Optional) Interface ID for the physical port (including type, stack member for stacking-capable switches, module, and port number).
broadcast	(Optional) Displays broadcast storm threshold setting.
multicast	(Optional) Displays multicast storm threshold setting.
unicast	(Optional) Displays unicast storm threshold setting.

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter an interface ID, the storm control thresholds appear for the specified interface.

If you do not enter an interface ID, settings appear for one traffic type for all ports on the switch.

If you do not enter a traffic type, settings appear for broadcast storm control.

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Device> show storm-control
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
Gi1/0/2   Forwarding    50.00%     40.00%    0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Device> show storm-control gigabitethernet 1/0/1
Interface Filter State  Upper      Lower     Current
--------- ------------- ---------- --------- ---------
Gi1/0/1   Forwarding    20 pps     10 pps    5 pps
```

The following table describes the fields in the show storm-control display:

Table 31: show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.
Filter State	Displays the status of the filter: • Blocking—Storm control is enabled, and a storm has occurred. • Forwarding—Storm control is enabled, and no storms have occurred. • Inactive—Storm control is disabled.
Upper	Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.

Field	Description
Lower	Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.
Current	Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled.

show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

show vlan access-map [*map-name*]

Syntax Description

map-name	(Optional) Name of a specific VLAN access map.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show vlan access-map** command:

```
Device# show vlan access-map
Vlan access-map "vmap4"  10
  Match clauses:
    ip  address: al2
  Action:
    forward
Vlan access-map "vmap4"  20
  Match clauses:
    ip  address: al2
  Action:
    forward
```

show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the **show vlan filter** command in privileged EXEC mode.

show vlan filter {**access-map** *name*| **vlan** *vlan-id*}

Syntax Description

access-map *name*	(Optional) Displays filtering information for the specified VLAN access map.
vlan *vlan-id*	(Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show vlan filter** command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *vlan-group-name* **[user_count]**]

Syntax Description

group-name *vlan-group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.
user_count	(Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Device# show vlan group group-name group2 user_count
  VLAN     : Count
-------------------
  40        : 5
  41        : 8
  42        : 12
  43        : 2
  44        : 9
  45        : 0
```

storm-control

To enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface, use the **storm-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

storm-control {**action** {**shutdown**| **trap**}| {**broadcast**| **multicast**| **unicast**} **level** {*level* [*level-low*]| **bps** *bps* [*bps-low*]| **pps** *pps* [*pps-low*]}}

no storm-control {**action** {**shutdown**| **trap**}| {**broadcast**| **multicast**| **unicast**} **level**}

Syntax Description

action	Specifies the action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs.
broadcast	Enables broadcast storm control on the interface.

multicast	Enables multicast storm control on the interface.
unicast	Enables unicast storm control on the interface.
level	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port.
level	Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for level is reached.
level-low	(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level.
level bps	Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.
bps	Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for bps is reached. You can use metric suffixes such as k, m, and g for large number thresholds.
bps-low	(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value. You can use metric suffixes such as k, m, and g for large number thresholds.
level pps	Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.
pps	Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for pps is reached. You can use metric suffixes such as k, m, and g for large number thresholds.
pps-low	(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value. You can use metric suffixes such as k, m, and g for large number thresholds.

Command Default

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.

Note When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the switch does not differentiate between routing updates, such as Open Shortest Path First (OSPF) and regular multicast data traffic, so both types of traffic are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

Note Storm control is supported on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

For more information, see the software configuration guide for this release.

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

```
Device(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Device(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Device(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Device(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the **switchport port-security aging** command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the **no** form of this command.

switchport port-security aging {**static**| **time** *time*| **type** {**absolute**| **inactivity**}}

no switchport port-security aging {**static**| **time**| **type**}

Syntax Description

static	Enables aging for statically configured secure addresses on this port.
time *time*	Specifies the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
type	Sets the aging type.
absolute	Sets absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
inactivity	Sets the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Command Default

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport port-security aging time 2
Device(config-if)# switchport port-security aging type inactivity
Device(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

To configure secure MAC addresses or sticky MAC address learning, use the **switchport port-security mac-address** interface configuration command. To return to the default setting, use the **no** form of this command.

switchport port-security mac-address {*mac-address* [**vlan** {*vlan-id* {**access**| **voice**}}]| **sticky** [*mac-address*| **vlan** {*vlan-id* {**access**| **voice**}}]}

no switchport port-security mac-address {*mac-address* [**vlan** {*vlan-id* {**access**| **voice**}}]| **sticky** [*mac-address*| **vlan** {*vlan-id* {**access**| **voice**}}]}

Syntax Description

mac-address	A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.
vlan *vlan-id*	(Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.
vlan access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
vlan voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.
sticky	Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.
mac-address	(Optional) A MAC address to specify a sticky secure MAC address.

Command Default

No secure MAC addresses are configured.

Sticky learning is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.
- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.

- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky** *mac-address* interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

To configure the maximum number of secure MAC addresses, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *value* [**vlan** [*vlan-list*| [**access**| **voice**]]]

no switchport port-security maximum *value* [**vlan** [*vlan-list*| [**access**| **voice**]]]

Syntax Description

value	Sets the maximum number of secure MAC addresses for the interface. The default setting is 1.
vlan	(Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the **vlan** keyword is not entered, the default value is used.
vlan-list	(Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN. **Note** The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

  Voice VLAN is supported only on access ports and not on trunk ports.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

  Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {**protect**| **restrict**| **shutdown**| **shutdown vlan**}

no switchport port-security violation {**protect**| **restrict**| **shutdown**| **shutdown vlan**}

Syntax Description

protect	Sets the security violation protect mode.
restrict	Sets the security violation restrict mode.
shutdown	Sets the security violation shutdown mode.
shutdown vlan	Sets the security violation mode to per-VLAN shutdown.

Command Default

The default violation mode is **shutdown**.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the security violation protect mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.

Note We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

In the security violation restrict mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

In the security violation shutdown mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.

When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

  A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

  When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command. You can manually re-enable the port by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface** privileged EXEC command.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
```

tracking (IPv6 snooping)

To override the default tracking policy on a port, use the **tracking** command in IPv6 snooping policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}

Syntax Description

enable	Enables tracking.

reachable-lifetime	(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through IPv6 snooping. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with

the tracking command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port

no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

ND inspection policy configuration

IPv6 snooping configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6  nd inspection  policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

wireless dot11-padding

To enable over-the-air frame padding, use the **wireless dot11-padding** command. To disable, use the **no** form of the command.

wireless dot11-padding

no wireless dot11-padding

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to enable over-the-air frame padding

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless dot11-padding
```

wireless security dot1x

To configure IEEE 802.1x global configurations, use the **wireless security dot1x** command.

wireless security dot1x [**eapol-key** {**retries** *retries*| **timeout** *milliseconds*}| **group-key interval** *sec*| **identity-request** {**retries** *retries*| **timeout** *seconds*}| **radius [call-station-id]** {**ap-macaddress**| **ap-macaddress-ssid**| **ipaddress**| **macaddress**}| **request** {**retries** *retries*| **timeout** *seconds*}| **wep key** {**index 0**| **index 3**}]

Syntax Description

eapol-key	Configures eapol-key related parameters.

retries *retries*	(Optional) 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.
timeout *milliseconds*	(Optional) 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.
group-key interval *sec*	Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request	Configures EAP ID request related parameters.
retries *retries*	(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout *seconds*	(Optional) 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.
radius	Configures radius messages.
call-station-id	(Optional) Configures Call-Station Id sent in radius messages.
ap-macaddress	Sets Call Station Id Type to the AP's MAC Address.
ap-macaddress-ssid	Sets Call Station Id Type to 'AP MAC address':'SSID'.
ipaddress	Sets Call Station Id Type to the system's IP Address.
macaddress	Sets Call Station Id Type to the system's MAC Address.
request	Configures EAP request related parameters.
retries *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.
timeout *seconds*	(Optional) 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.
wep key	Configures 802.1x WEP related paramters.

index 0	Specifies the WEP key index value as 0
index 3	Specifies the WEP key index value as 3

Command Default

Default for eapol-key-timeout: 1 second.

Default for eapol-key-retries: 2 retries.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example lists all the commands under **wireless security dot1x** .

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security dot1x ?
  eapol-key         Configure eapol-key related parameters
  group-key         Configures EAP-broadcast key renew interval time in seconds
  identity-request  Configure EAP ID request related parameters
  radius            Configure radius messages
  request           Configure EAP request related parameters
  wep               Configure 802.1x WEP related paramters
  <cr>
```

wireless security lsc

To configure locally significant certificates, use the **wireless security lsc** command.

wireless security lsc {**ap-provision** [**auth-list** *mac-addr*| **revert** *number*]| **other-params** *key-size*| **subject-params** *country state city orgn dept email*| **trustpoint** *trustpoint*}

Syntax Description

ap-provision	Specifies the access point provision list settings.
auth-list *mac-addr*	Specifies the provision list authorization settings.
revert *number*	Specifies the number of times the access point attempts to join the controller using an LSC before reverting to the default certificate. The maximum number of attempts cannot exceed 255.
other-params *key-size*	Specifies the device certificate key size settings.

subject-params *country state city orgn dept email*	Specifies the device certificate settings. Country, state, city, organization, department, and email of the certificate authority.
trustpoint *trustpoint*	Specifies the LSC Trustpoint.

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

This example shows how to configure locally significant certificate:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security lsc ?
  ap-provision    Provisioning the AP's with LSC's
  other-params    Configure Other Parameters for Device Certs
  subject-params  Configure the Subject Parameters for Device Certs
  trustpoint      Configure LSC Trustpoint
  <cr>
```

wireless security strong-password

To configure strong password enforcement options, use the **wireless security strong-password** command. To disable strong password, use the no form of the command.

wireless security strong-password

no wireless security strong-password

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to configure a strong-password for wireless security.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless security strong-password
```

wireless wps ap-authentication

To configure the access point neighbor authentication, use the **wireless wps ap-authentication** command. To remove the access point neighbor authentication, use the no form of the command.

wireless wps ap-authentication [**threshold** *value*]

no wireless wps ap-authentication [threshold]

Syntax Description

threshold *value*	Specifies that the WMM-enabled clients are on the wireless LAN. Threshold value (1 to 255).

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to set the threshold value for WMM-enabled clients.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps ap-authentication threshold 65
```

wireless wps auto-immune

To enable protection from denial of service (DoS) attacks, use the **wireless wps auto-immune** command. To disable, use the no form of the command.

wireless wps auto-immune

no wireless wps auto-immune

Command Default

Disabled.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

This example shows how to enable protection from denial of service (DoS) attack:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps auto-immune
```

wireless wps cids-sensor

To configure Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the **wireless wps cids-sensor** command. To remove the Intrusion Detection System (IDS) sensors for the Wireless Protection System (WPS), use the no form of the command.

wireless wps cids-sensor *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]

no wireless wps cids-sensor *index*

Syntax Description

index	Specifies the IDS sensor internal index.
ip-address *ip-addr* **username** *username* **password** *password_type password*	Specifies the IDS sensor IP address, IDS sensor username, password type and IDS sensor password.

Command Default Disabled.

Command Modes config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines None

This example shows how to configure the Intrusion Detection System with the IDS index, IDS sensor IP address, IDS username and IDS password.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps cids-sensor 1 10.0.0.51 Sensor_user0doc1 passowrd01
```

wireless wps client-exclusion

To configure client exclusion policies, use the **wireless wps client-exclusion** command. To remove the client exclusion policies, use the **no** form of the command.

wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

no wireless wps client-exclusion {**all**| **dot11-assoc**| **dot11-auth**| **dot1x-auth**| **ip-theft**| **web-auth**}

Syntax Description

dot11-assoc	Specifies that the controller excludes clients on the sixth 802.11 association attempt, after five consecutive failures.
dot11-auth	Specifies that the controller excludes clients on the sixth 802.11 authentication attempt, after five consecutive failures.
dot1x-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. For more information, see the Usage Guidelines section.
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.

Command Default Enabled.

Command Modes config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines In IP-theft scenarios, there are differences between the older Cisco IOS XE releases and the Cisco IOS XE Denali 16.x releases:

Older Cisco IOS XE Releases	Cisco IOS XE Denali 16.x Releases
Priority wise, wired clients have higher priority over wireless clients, and DHCP IP has higher priority over static IP. The client security type is not checked; security of all client types are treated with same priority. If the existing binding is from a higher priority source, the new binding is ignored and an IP-theft is signaled. If the existing binding has the same source-priority as the new binding, the binding is ignored and an IP-theft is signaled. This ensures that the bindings are not toggled if two hosts send traffic using the same IP. Only the initial binding is retained in the software. If the new binding is from a higher priority source, the existing binding is replaced. This results in an IP-theft notification of existing binding and also a new binding notification.	There is not really a fundamental difference between wired and wireless; what matters is the trust (preflevel) of the entry, which is a function on how it was learnt (ARP, DHCP, ND, and so on) and the policy that is attached to the port. When preflevel is equal, the IP takeover is denied if the old entry is still reachable. IP takeover occurs when the update comes from a trusted port or a new entry gets IP from the DHCP server. Otherwise, you must explicitly grant it. The IP-theft is not reported if an old entry is replaced by a new and a more trusted one.

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps client-exclusion dot11-assoc
```

wireless wps mfp infrastructure

To configure Management Frame Protection (MFP), use the **wireless wps mfp infrastructure** command. To remove the Management Frame Protection (MFP), use the no form of the command.

wireless wps mfp infrastructure

no wireless wps mfp infrastructure

Command Default

None.

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to enable the infrastructure MFP.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps mfp infrastructure
```

wireless wps rogue

To configure various rouge parameters, use the **wireless wps rogue** command.

wireless wps rogue {**adhoc**| **client**} [**alert** *mac-addr*| **contain** *mac-addr no-of-aps*]

Syntax Description

adhoc	Configures the status of an Independent Basic Service Set (IBSS or ad-hoc) rogue access point.
client	Configures rogue clients
alert *mac-addr*	Generates an SNMP trap upon detection of the ad-hoc rogue, and generates an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.
contain *mac-addr no-of-aps*	Contains the offending device so that its signals no longer interfere with authorized clients. Maximum number of Cisco access points assigned to actively contain the ad-hoc rogue access point (1 through 4, inclusive).

Command Default

None.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to generate an immediate alert to the system administrator for further action for the MAC address of the ad-hoc rogue access point.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps rouge adhoc alert mac_addr
```

wireless wps shun-list re-sync

To force the controller to synchronization with other controllers in the mobility group for the shun list, use the **wireless wps shun-list re-sync** command.

wireless wps shun-list re-sync

Command Default

None.

Command Modes

Any command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

None.

This example shows how to configure the controller to synchronize with other controllers for the shun list.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless wps shun-list re-sync
```

vlan access-map

To create or modify a VLAN map entry for VLAN packet filtering, and change the mode to the VLAN access-map configuration, use the **vlan access-map** command in global configuration mode on the switch stack or on a standalone switch. To delete a VLAN map entry, use the **no** form of this command.

vlan access-map *name* [*number*]

no vlan access-map *name* [*number*]

Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

name	Name of the VLAN map.
number	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action—**Sets the action to be taken (forward or drop).
- **default—**Sets a command to its defaults.
- **exit—**Exits from VLAN access-map configuration mode.
- **match—**Sets the values to match (IP address or MAC address).
- **no—**Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1
Device(config-access-map)# match ip address acl1
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Device(config)# no vlan access-map vac1
```

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

vlan filter *mapname* **vlan-list** {*list*| **all**}

no vlan filter *mapname* **vlan-list** {*list*| **all**}

Note This command is not supported on switches running the LAN Base feature set.

Syntax Description

mapname	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
list	The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Device(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*

no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
vlan-list *vlan-list*	Specifies one or more VLANs to be added to the VLAN group. The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```

PART XIII

Stack Manager and High Availability

- Stack Manager and High Availability Commands, page 761

CHAPTER 14

Stack Manager and High Availability Commands

- debug platform stack-manager, page 762
- main-cpu, page 763
- mode sso, page 763
- policy config-sync prc reload, page 764
- redundancy, page 765
- redundancy config-sync mismatched-commands, page 766
- redundancy force-switchover, page 767
- redundancy reload, page 768
- reload, page 769
- session, page 770
- set trace capwap ap ha, page 771
- set trace mobility ha, page 772
- set trace qos ap ha, page 774
- show checkpoint, page 775
- show etherchannel summary, page 780
- show platform ses, page 781
- show platform stack-manager, page 786
- show redundancy, page 787
- show redundancy config-sync, page 790
- show switch, page 792
- show trace messages capwap ap ha, page 796
- show trace messages mobility ha, page 797
- stack-mac persistent timer, page 798
- stack-mac update force, page 799

- standby console enable, page 800
- switch stack port, page 801
- switch priority, page 802
- switch provision, page 802
- switch renumber, page 804

debug platform stack-manager

To enable debugging of the stack manager software, use the **debug platform stack-manager** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform stack-manager {**level1**| **level2**| **level3**| **sdp**| **serviceability**| **sim**| **ssm**| **trace**} [**switch** *switch-number*]

no debug platform stack-manager {**level1**| **level2**| **level3**| **sdp**| **serviceability**| **sim**| **ssm**| **trace**} [**switch** *switch-number*]

Syntax Description

level1	Enables level 1 debug logs.
level2	Enables level 2 debug logs.
level3	Enables level 3 debug logs.
sdp	Displays the Stack Discovery Protocol (SDP) debug messages.
serviceability	Displays stack manager serviceability debug messages.
sim	Displays the stack information module debug messages.
ssm	Displays the stack state-machine debug messages.
trace	Traces the stack manager entry and exit debug messages.
switch *switch-number*	(Optional) Specifies the stack member number to enable debugging on. The range is 1 to 9.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is supported only on stacking-capable switches.

The **undebug platform stack-manager** command is the same as the **no debug platform stack-manager** command.

main-cpu

To enter the redundancy main configuration submode and enable the standby switch, use the **main-cpu** command in redundancy configuration mode.

main-cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

From the redundancy main configuration submode, use the **standby console enable** command to enable the standby switch.

This example shows how to enter the redundancy main configuration submode and enable the standby switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

mode sso

To set the redundancy mode to stateful switchover (SSO), use the **mode sso** command in redundancy configuration mode.

mode sso

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **mode sso** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to SSO mode:

- You must use identical Cisco IOS images on the switches in the stack to support SSO mode. Redundancy may not work due to differences between the Cisco IOS releases.
- If you perform an online insertion and removal (OIR) of the module, the switch resets during the stateful switchover and the port states are restarted only if the module is in a transient state (any state other than Ready).
- The forwarding information base (FIB) tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

This example shows how to set the redundancy mode to SSO:

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)#
```

policy config-sync prc reload

To reload the standby switch if a parser return code (PRC) failure occurs during configuration synchronization, use the **policy config-sync reload** command in redundancy configuration mode. To specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs, use the **no** form of this command.

policy config-sync {**bulk**| **lbl**} **prc reload**

no policy config-sync {**bulk**| **lbl**} **prc reload**

Syntax Description

bulk	Specifies bulk configuration mode.
lbl	Specifies line-by-line (lbl) configuration mode.

Command Default

The command is enabled by default.

Command Modes

Redundancy configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs during configuration synchronization:

```
Device(config-red)# no policy config-sync bulk prc reload
```

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The redundancy configuration mode is used to enter the main CPU submode, which is used to enable the standby switch.

To enter the main CPU submode, use the **main-cpu** command while in redundancy configuration mode.

From the main CPU submode, use the **standby console enable** command to enable the standby switch.

Use the **exit** command to exit redundancy configuration mode.

This example shows how to enter redundancy configuration mode:

```
Device(config)# redundancy
Device(config-red)#
```

This example shows how to enter the main CPU submode:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)#
```

redundancy config-sync mismatched-commands

To allow the standby switch to join the stack if a configuration mismatch occurs between the active and standby switches, use the **redundancy config-sync mismatched-commands** command in privileged EXEC mode.

redundancy config-sync {**ignore**| **validate**} **mismatched-commands**

Syntax Description

ignore	Ignores the mismatched command list.
validate	Revalidates the mismatched command list with the modified running-configuration.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If the command syntax check in the running configuration of the active switch fails while the standby switch is booting, use the **redundancy config-sync mismatched-commands** command to display the Mismatched Command List (MCL) on the active switch and to reboot the standby switch.

The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1 Remove all mismatched commands from the running configuration of the active switch.

2 Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.

3 Reload the standby switch.

You can ignore the MCL by doing the following:

1 Enter the **redundancy config-sync ignore mismatched-commands** command.

2 Reload the standby switch; the system changes to SSO mode.

Note If you ignore the mismatched commands, the out-of-sync configuration at the active switch and the standby switch still exists.

3 Verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

If SSO mode cannot be established between the active and standby switches because of an incompatibility in the configuration file, a mismatched command list (MCL) is generated at the active switch and a reload into route processor redundancy (RPR) mode is forced for the standby switch.

Note RPR mode is supported on Catalyst 3850 switches as a fallback in case of errors. It is not configurable.

If you attempt to establish an SSO after removing the offending configuration and rebooting the standby switch with the same image, the C3K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL and ISSU-3-PEER_IMAGE_INCOMPATIBLE messages appear because the peer image is listed as incompatible. You can clear the peer image from the incompatible list with the **redundancy config-sync ignore mismatched-commands** EXEC command while the peer is in a standby cold (RPR) state. This action allows the standby switch to boot in a standby hot (SSO) state when it reloads.

This example shows how to revalidate the mismatched command list with the modified configuration:

```
Device# redundancy config-sync validate mismatched-commands
Device#
```

redundancy force-switchover

To force a switchover from the active switch to the standby switch, use the **redundancy force-switchover** command in privileged EXEC mode on a switch stack.

redundancy force-switchover

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **redundancy force-switchover** command to manually switch over to the redundant switch. The redundant switch becomes the new active switch that runs the Cisco IOS image, and the modules are reset to their default settings.

The old active switch reboots with the new image and joins the stack.

If you use the **redundancy force-switchover** command on the active switch, the switchports on the active switch to go down.

If you use this command on a switch that is in a partial ring stack, the following warning message appears:

```
Device# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

This example shows how to manually switch over from the active to the standby supervisor engine:

```
Device# redundancy force-switchover
Device#
```

redundancy reload

To force a reload of one or all of the switches in the stack, use the **redundancy reload** command in privileged EXEC mode.

redundancy reload {**peer**| **shelf**}

Syntax Description

peer	Reloads the peer unit.
shelf	Reboots all switches in the stack.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before using this command, see the "Performing a Software Upgrade" section of the *Stacking Configuration Guide (Catalyst 3850 Switches)* for additional information.

Use the **redundancy reload shelf** command to reboot all the switches in the stack.

This example shows how to manually reload all switches in the stack:

```
Device# redundancy reload shelf
Device#
```

reload

To reload the stack member and to apply a configuration change, use the **reload** command in privileged EXEC mode.

reload [**/noverify**| **/verify**] [*LINE*| **at**| **cancel**| **in**| **slot** *stack-member-number*| **standby-cpu**]

Syntax Description

/noverify	(Optional) Specifies to not verify the file signature before the reload.
/verify	(Optional) Verifies the file signature before the reload.
LINE	(Optional) Reason for the reload.
at	(Optional) Specifies the time in hh:mm for the reload to occur.
cancel	(Optional) Cancels the pending reload.
in	(Optional) Specifies a time interval for reloads to occur.
slot	(Optional) Saves the changes on the specified stack member and then restarts it.
stack-member-number	(Optional) Stack member number on which to save the changes. The range is 1 to 9.
standby-cpu	(Optional) Reloads the standby route processor (RP).

Command Default

Immediately reloads the stack member and puts a configuration change into effect.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If there is more than one switch in the switch stack, and you enter the **reload slot** *stack-member-number* command, you are not prompted to save the configuration.

This example shows how to reload the switch stack:

```
Device# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

This example shows how to reload a specific stack member:

```
Device# reload slot 6
Proceed with reload? [confirm] y
```

This example shows how to reload a single-switch switch stack (there is only one member switch):

```
Device# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

session

To access the diagnostic shell of a specific stack member or to access the Cisco IOS prompt of the standby Device use the **session** command in privileged EXEC mode on the active Device.

session {**standby ios**| **switch** [*stack-member-number*]}

Syntax Description

standby ios	Accesses the Cisco IOS prompt of the standby Device. **Note** You cannot configure the standby Device using this command.
switch	Accesses the diagnostic shell of a stack member.
stack-member-number	(Optional) Stack member number to access from the active switch. The range is 1 to 9.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you access the Cisco IOS prompt on the standby Device, `-stby` is appended to the system prompt. You cannot configure the standby Device at the `Device-stby>` prompt.

When you access the diagnostic shell of a stack member, `(diag)` is appended to the system prompt.

This example shows how to access stack member 3:

```
Device# session switch 3
Device(diag)>
```

This example shows how to access the standby Device:

```
Device# session standby ios
Device-stby>
```

set trace capwap ap ha

To trace the control and provisioning of wireless access point high availability, use the **set trace capwap ap ha** privileged EXEC command.

set trace capwap ap ha [**detail**| **event**| **dump** | {**filter** [**none** [**switch** *switch*]|*filter_name* [*filter_value* [**switch** *switch*]]]| **filtered***switch***level** {**default**| *trace_level*} [**switch** *switch*]}]

Syntax Description

detail	(Optional) Specifies the wireless CAPWAP HA details.
event	(Optional) Specifies the wireless CAPWAP HA events.
dump	(Optional) Specifies the wireless CAPWAP HA output.
filter *mac*	Specifies the MAC address.
switch switch number	Specifies the switch number.
none	(Optional) Specifies the no filter option.
switch *switch*	(Optional) Specifies the device number.
filter name	Trace adapted flag filter name.
filter_value	(Optional) Value of the filter.
switch *switch*	(Optional) Specifies the device number.
filtered	Specifies the filtered traces messages.
switch	Specifies the switch number.
level	Specifies the trace level.
default	Specifies the unset trace level value.

trace_level	Specifies the trace level.
switch *switch*	(Optional) Specifies the device number.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display the wireless CAPWAP HA:

```
Device# set trace capwap ap ha detail filter mac WORD switch number
```

set trace mobility ha

To debug the wireless mobility high availability in the switch, use the **set trace mobility ha** privileged EXEC command.

set trace mobility ha [**event**| **detail**| **dump**] {**filter**[**mac** *WORD switch switch number*] [**none** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]{**filtered**| *switch*}}

Syntax Description

event	(Optional) Specifies the wireless mobility high availability events.
detail	(Optional) Specifies the wireless mobility high availability details.
dump	(Optional) Specifies the wireless mobility high availability output.
filter	Specifies to trace adapted flag filter.
mac	Specifies the MAC address.
WORD switch	Specifies the switch.
switch number	Specifies the switch number. The value ranges from one to four.

none	Specifies no trace adapted flag filter.
switch *switch*	(Optional) Specifies the device number.
filter_name	Trace adapted flag filter name.
filter_value	Trace adapted flag filter value.
switch *switch*	Specifies the device number.
level	Specifies the trace level value.
default	Specifies the un-set trace level value.
trace_level	Specifies the trace level value.
switch *switch*	Specifies the device number.
filtered	Specifies the filtered trace messages.
switch	Specifies the switch.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display wireless mobility high availability details:

```
Device# set trace mobility ha detail filter mac WORD
[08/27/13 10:38:35.349 UTC 1 8135] Invalid src ip: 169.254.1.1
[08/27/13 10:38:35.349 UTC 2 8135] Invalid sysIp: Skip plumbing MC-MA
tunnels.
[08/27/13 10:38:54.393 UTC 3 8135] Mobility version mismatch, v10 received,
 or m
sglen mismatch msglen=74 recvBytes=0, dropping
```

set trace qos ap ha

To trace wireless Quality of Service (QoS) high availability, use the **set trace qos ap ha** privileged EXEC command.

set trace QOS ap ha [**event**| **error**] {**filter** [**MACnone** [**switch** *switch*]| *filter_name* [*filter_value* [**switch** *switch*]]]| **level** {**default**| *trace_level*} [**switch** *switch*]}

Syntax Description

event	(Optional) Specifies trace QoS wireless AP event.
event *mac*	Specifies the MAC address of the AP.
event *none*	Specifies no MAC address value.
error	(Optional) Specifies trace QoS wireless AP errors.
error *mac*	Specifies the MAC address of the AP.
error *none*	Specifies no value.
filter	Specifies the trace adapted flag filter.
filter *mac*	Specifies the MAC address of the AP.
filter *none*	Specifies no value.
switch *switch*	Specifies the switch number.
filter_name	(Optional) Specifies the switch filter name.
filter_value	(Optional) Specifies the switch filter value. Value is one.
switch *switch*	(Optional) Specifies the switch number. Value is one.
level	Specifies the trace level.
default	Specifies the trace QoS wireless AP default.
trace_level	Trace level.
switch *switch*	(Optional) Specifies the switch number. Value is one.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to trace wireless QoS high availability:

```
Device# set trace QOS ap ha
```

show checkpoint

To display information about the Checkpoint Facility (CF) subsystem, use the **show checkpoint** command.

show checkpoint clients entities statistics

Syntax Description

clients	Displays detailed information about checkpoint clients.
entities	Displays detailed information about checkpoint entities.
statistics	Displays detailed information about checkpoint statistics.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display all the CF clients.

```
   Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_MOBILITY
    Client ID                  : 24105
    Total DB inserts           : 0
    Total DB updates           : 0
    Total DB deletes           : 0
    Total DB reads             : 0
    Number of tables           : 6
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_DOT1X
    Client ID                  : 24106
    Total DB inserts           : 2
    Total DB updates           : 1312
    Total DB deletes           : 2
```

```
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_APFROGUE
    Client ID                   : 24107
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_CIDS
    Client ID                   : 24110
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_NETFLOW
    Client ID                   : 24111
    Total DB inserts            : 7
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: WCM_MCAST
    Client ID                   : 24112
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 1
    Client residing in process  : 8135
-------------------------------------------------------------------------------
Checkpoint client: wcm_comet
    Client ID                   : 24150
    Total DB inserts            : 0
    Total DB updates            : 0
    Total DB deletes            : 0
    Total DB reads              : 0
    Number of tables            : 0
    Client residing in process  : 8135
-------------------------------------------------------------------------------

All iosd checkpoint clients

-------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                          ID         ID       Mode
-------------------------------------------------------------------------------
Network RF Client           3         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
```

```
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
SNMP CF Client             12         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Online Diags HA            14         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
ARP                        22         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
```

```
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Tableid CF                 27         --       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                 0
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
Event Manager              33          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
--------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
--------------------------------------------------------------------------------
LAN-Switch Port Mana       35          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
```

```
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
-------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
-------------------------------------------------------------------------------
LAN-Switch PAgP/LACP       36          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
  Xmit Xform Errs:                               0
  Incompatible Messages:                         0
  Client Unbundles to Process Memory:            T
-------------------------------------------------------------------------------
Client Name            Client     Entity     Bundle
                           ID         ID       Mode
-------------------------------------------------------------------------------
LAN-Switch VLANs           39          0       Off

  Total API Messages Sent:                       0
  Total Transport Messages Sent:                --
  Length of Sent Messages:                       0
  Total Blocked Messages Sent:                   0
  Length of Sent Blocked Messages:               0
  Total Non-blocked Messages Sent:               0
  Length of Sent Non-blocked Messages:           0
  Total Bytes Allocated:                         0
  Buffers Held:                                  0
  Buffers Held Peak:                             0
  Huge Buffers Requested:                        0
  Transport Frag Count:                          0
  Transport Frag Peak:                           0
  Transport Sends w/Flow Off:                    0
  Send Errs:                                     0
  Send Peer Errs:                                0
  Rcv Xform Errs:                                0
```

This example shows how to display all the CF entities.

```
KATANA_DOC#show checkpoint entities
                         Check Point List of Entities

 CHKPT on ACTIVE server.
```

```
-------------------------------------------------------------------------------
Entity ID         Entity Name
-------------------------------------------------------------------------------
        0         CHKPT_DEFAULT_ENTITY

  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Total Number of Members:            10

  Member(s) of entity 0 are:
    Client ID          Client Name
-----------------------------------------
          168          DHCP Snooping
          167          IGMP Snooping
           41          Spanning-tree
           40          AUTH MGR CHKPT CLIEN
           39          LAN-Switch VLANs
           33          Event Manager
           35          LAN-Switch Port Mana
           36          LAN-Switch PAgP/LACP
          158          Inline Power Checkpoint
```

This example shows how to display the CF statistics.

```
KATANA_DOC#show checkpoint statistics
        IOSd Check Point Status
 CHKPT on ACTIVE server.

Number Of Msgs In Hold Q:              0
CHKPT MAX Message Size:                0
TP MAX Message Size:               65503
CHKPT Pending Msg Timer:             100 ms

  FLOW_ON  total:                      0
  FLOW_OFF total:                      0
  Current FLOW status is:             ON
  Total API Messages Sent:             0
  Total Messages Sent:                 0
  Total Sent Message Len:              0
  Total Bytes Allocated:               0
  Rcv  Msg Q Peak:                     0
  Hold Msg Q Peak:                     0
  Buffers Held Peak:                   0
  Current Buffers Held:                0
  Huge Buffers Requested:              0
```

show etherchannel summary

To show details on the ports, port-channel, and protocols in the controller, use the **show etherchannel summary** command.

show ethernet summary

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged Mode.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows the details on the ports, port-channel, and protocols in the controller.

```
controller#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
2      Po2(SD)          -
23     Po23(SD)         -
```

show platform ses

To display the platform information - the stack event sequencer in the controller, use the **show platform ses** in the privileged EXEC mode.

show platform ses clients states

Syntax Description

clients	Displays the SES client list.
states	Displays the SES card states.

Command Default

None.

Command Modes

Privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use this command in the privileged EXEC mode to view the ses clients and states detail.

This example shows the stack event sequencer states.

```
Card #  Card State
======  ==========
1       NG3K_SES_CARD_ADD_COMPLETED(51)
2       NG3K_SES_CARD_EMPTY(0)
3       NG3K_SES_CARD_EMPTY(0)
4       NG3K_SES_CARD_EMPTY(0)
5       NG3K_SES_CARD_EMPTY(0)
6       NG3K_SES_CARD_EMPTY(0)
7       NG3K_SES_CARD_EMPTY(0)
8       NG3K_SES_CARD_EMPTY(0)
9       NG3K_SES_CARD_EMPTY(0)
```

This example shows all the associated clients of the stack event sequencer.

```
clientID  = 5
clientSeq = 5
clientName = "MATM"
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0

clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C
```

```
clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728

clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
clientSeq = 23
clientName = "LEARNING"
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144
```

```
clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000

KATANA_DOC#
KATANA_DOC#
KATANA_DOC#show platform ses clients
Client list @ 0x915B312C

clientID  = 0
clientSeq = 0
clientName = "TM Shim"
clientCallback @ 0xF4C79A90
next = 0x91182F24

clientID  = 1
clientSeq = 1
clientName = "EM-HA"
clientCallback @ 0xF52CA730
next = 0x913245B8

clientID  = 2
clientSeq = 2
clientName = "IFM"
clientCallback @ 0xF4A3EB20
next = 0x934B80E4

clientID  = 3
clientSeq = 3
clientName = "PORT-MGR"
clientCallback @ 0xF49FD0A0
next = 0x91D36D08

clientID  = 4
clientSeq = 4
clientName = "IDBMAN"
clientCallback @ 0xF4AF6040
next = 0x92121224

clientID  = 5
clientSeq = 5
clientName = "MATM"
clientCallback @ 0xF49F7300
next = 0x909194B4

clientID  = 6
clientSeq = 6
clientName = "L2 CONTROL"
clientCallback @ 0xF49CA3F0
next = 0x915E4E80

clientID  = 7
clientSeq = 7
clientName = "CDP"
clientCallback @ 0xF49C7220
next = 0x915E4F08

clientID  = 8
clientSeq = 8
clientName = "UDLD"
clientCallback @ 0xF49C75D0
next = 0x91854CA0

clientID  = 9
clientSeq = 9
clientName = "LLDP"
clientCallback @ 0xF49E62F0
next = 0x90919F90

clientID  = 10
clientSeq = 10
```

```
clientName = "L2M"
clientCallback @ 0xF49CE4D0
next = 0x90E35A5C

clientID  = 11
clientSeq = 11
clientName = "Storm-Control"
clientCallback @ 0xF4BA8080
next = 0x9089E9B4

clientID  = 12
clientSeq = 12
clientName = "Security Utils"
clientCallback @ 0xF466BFB0
next = 0x91855F14

clientID  = 13
clientSeq = 13
clientName = "BACKUP-INT"
clientCallback @ 0xF4A191B0
next = 0x91D3511C

clientID  = 14
clientSeq = 14
clientName = "SPAN"
clientCallback @ 0xF4A34F30
next = 0x90FFC8C8

clientID  = 15
clientSeq = 15
clientName = "NG3K_SES_CLIENT_SECURITY_CTRL"
clientCallback @ 0xF4CD1D80
next = 0x95AE5834

clientID  = 16
clientSeq = 16
clientName = "NG3K_SES_CLIENT_DAI"
clientCallback @ 0xF4CD0C50
next = 0x95AE4854

clientID  = 17
clientSeq = 17
clientName = "NG3K_SES_CLIENT_DHCPSN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728

clientID  = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CDED70
next = 0x9131DCD8

clientID  = 20
clientSeq = 20
clientName = "DTLS"
clientCallback @ 0xF49B2CB0
next = 0x9134508C

clientID  = 21
clientSeq = 21
clientName = "STATS"
clientCallback @ 0xF49BD750
next = 0x9134746C

clientID  = 22
clientSeq = 22
clientName = "PLATFORM_MGR"
clientCallback @ 0xF4AB2D40
next = 0x91323D20

clientID  = 23
clientSeq = 23
clientName = "LEARNING"
```

```
clientCallback @ 0xF49F93C0
next = 0x9091D52C

clientID  = 24
clientSeq = 24
clientName = "PLATFORM-SPI"
clientCallback @ 0xF4AAD6F0
next = 0x91F2AE14

clientID  = 25
clientSeq = 25
clientName = "EEM"
clientCallback @ 0xF5393370
next = 0x913474F4

clientID  = 26
clientSeq = 26
clientName = "NG3K_WIRELESS"
clientCallback @ 0xF4B130B0
next = 0x9131D144

clientID  = 27
clientSeq = 27
clientName = "NG3K Environment Variables"
clientCallback @ 0xF4C6DA80
next = 0x00000000
```

show platform stack-manager

To display platform-dependent switch-stack information, use the **show platform stack-manager** command in privileged EXEC mode.

show platform stack-manager {**oir-states**| **sdp-counters**| **sif-counters**} **switch** *stack-member-number*

Syntax Description

oir-states	Displays Online Insertion and Removal (OIR) state information
sdp-counters	Displays Stack Discovery Protocol (SDP) counter information.
sif-counters	Displays Stack Interface (SIF) counter information.
switch *stack-member-number*	Specifies the stack member for which to display stack-manager information.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show platform stack-manager** command to collect data and statistics for the switch stack.

Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

show redundancy

To display redundancy facility information, use the **show redundancy** command in privileged EXEC mode

show redundancy [**clients**| **config-sync**| **counters**| **history** [**reload**| **reverse**]| **slaves**[*slave-name*] {**clients**| **counters**}| **states**| **switchover history** [**domain default**]]

Syntax Description

clients	(Optional) Displays information about the redundancy facility client.
config-sync	(Optional) Displays a configuration synchronization failure or the ignored mismatched command list (MCL). For more information, see show redundancy config-sync, on page 790.
counters	(Optional) Displays information about the redundancy facility counter.
history	(Optional) Displays a log of past status and related information for the redundancy facility.
history reload	(Optional) Displays a log of past reload information for the redundancy facility.
history reverse	(Optional) Displays a reverse log of past status and related information for the redundancy facility.
slaves	(Optional) Displays all slaves in the redundancy facility.
slave-name	(Optional) The name of the redundancy facility slave to display specific information for. Enter additional keywords to display all clients or counters in the specified slave.
clients	Displays all redundancy facility clients in the specified slave.
counters	Displays all counters in the specified slave.
states	(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.
switchover history	(Optional) Displays information about the redundancy facility switchover history.
domain default	(Optional) Displays the default domain as the domain to display switchover history for.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display information about the redundancy facility:

```
Device# show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = not known

                 Hardware Mode = Simplex
    Configured Redundancy Mode = SSO
     Operating Redundancy Mode = SSO
              Maintenance Mode = Disabled
                Communications = Down      Reason: Simplex mode

Current Processor Information :
-------------------------------
               Active Location = slot 1
        Current Software state = ACTIVE
       Uptime in current state = 6 days, 9 hours, 23 minutes
                 Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
        Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
Device#
```

This example shows how to display redundancy facility client information:

```
Device# show redundancy clients
Group ID =     1
     clientID = 20002    clientSeq =     4    EICORE HA Client
     clientID = 24100    clientSeq =     5    WCM_CAPWAP
     clientID = 24101    clientSeq =     6    WCM RRM HA
     clientID = 24103    clientSeq =     8    WCM QOS HA
     clientID = 24105    clientSeq =    10    WCM_MOBILITY
     clientID = 24106    clientSeq =    11    WCM_DOT1X
     clientID = 24107    clientSeq =    12    WCM_APFROGUE
     clientID = 24110    clientSeq =    15    WCM_CIDS
     clientID = 24111    clientSeq =    16    WCM_NETFLOW
     clientID = 24112    clientSeq =    17    WCM_MCAST
     clientID = 24120    clientSeq =    18    wcm_comet
     clientID = 24001    clientSeq =    21    Table Manager Client
     clientID = 20010    clientSeq =    24    SNMP SA HA Client
     clientID = 20007    clientSeq =    27    Installer HA Client
     clientID =    29    clientSeq =    60    Redundancy Mode RF
     clientID =   139    clientSeq =    61    IfIndex
     clientID =  3300    clientSeq =    62    Persistent Variable
```

```
     clientID =    25    clientSeq =    68    CHKPT RF
     clientID = 20005    clientSeq =    74    IIF-shim
     clientID = 10001    clientSeq =    82    QEMU Platform RF

<output truncated>
```

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Device# show redundancy counters
Redundancy Facility OMs

               comm link up = 0
             comm link down = 0
          invalid client tx = 0
          null tx by client = 0
                tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
 rx peer msg routing errors = 0
           null peer msg rx = 0
        errored peer msg rx = 0

                 buffers tx = 0
     tx buffers unavailable = 0
                 buffers rx = 0
      buffer release errors = 0

 duplicate client registers = 0
  failed to register client = 0
       Invalid client syncs = 0

Device#
```

This example shows how to display redundancy facility history information:

```
Device# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM_QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM_RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDS(24110) seq=15
00:00:09 client added: wcm_comet(24120) seq=18
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) First Slave(0) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6107) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6109) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(6128) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8897) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8898) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Slave(8901) op=0 rc=0
00:00:22 RF_EVENT_SLAVE_STATUS_DONE(523) First Slave(0) op=405 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) Redundancy Mode RF(29) op=0 rc=0
00:00:22 RF_STATUS_REDUNDANCY_MODE_CHANGE(405) IfIndex(139) op=0 rc=0
```

```
<output truncated>
```

This example shows how to display information about the redundancy facility slaves:

```
Device# show redundancy slaves
Group ID =   1
Slave/Process ID =  6107   Slave Name = [installer]
Slave/Process ID =  6109   Slave Name = [eicored]
Slave/Process ID =  6128   Slave Name = [snmp_subagent]
Slave/Process ID =  8897   Slave Name = [wcm]
Slave/Process ID =  8898   Slave Name = [table_mgr]
Slave/Process ID =  8901   Slave Name = [iosd]

Device#
```

This example shows how to display information about the redundancy facility state:

```
Device# show redundancy states
         my state = 13 -ACTIVE
       peer state =  1 -DISABLED
            Mode = Simplex
          Unit ID = 1

  Redundancy Mode (Operational) = SSO
   Redundancy Mode (Configured) = SSO
               Redundancy State = Non Redundant
                      Manual Swact = disabled (system is simplex (no peer unit))

   Communications = Down      Reason: Simplex mode

     client count = 75
   client_notification_TMR = 360000 milliseconds
            keep_alive TMR = 9000 milliseconds
          keep_alive count = 0
      keep_alive threshold = 18
            RF debug mask = 0

Device#
```

show redundancy config-sync

To display a configuration synchronization failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command in EXEC mode.

show redundancy config-sync {**failures** {**bem**| **mcl**| **prc**}| **ignored failures mcl**}

Syntax Description

failures	Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.
bem	Displays a BEM failed command list, and forces the standby switch to reboot.
mcl	Displays commands that exist in the switch's running configuration but are not supported by the image on the standby switch, and forces the standby switch to reboot.
prc	Displays a PRC failed command list and forces the standby switch to reboot.
ignored failures mcl	Displays the ignored MCL failures.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active switch, the standby switch might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby switch during a bulk synchronization, the command is moved into the MCL and the standby switch is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the active switch's running configuration.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby switch.

Alternatively, you could ignore the MCL by following these steps:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby switch; the system transitions to SSO mode.

Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active switch and the standby switch still exists.

3. You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active switch maintains the PRC after executing a command. The standby switch executes the command and sends the PRC back to the active switch. A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby switch either during bulk synchronization or line-by-line (LBL) synchronization, the standby switch is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

This example shows how to display the BEM failures:

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----------------------

 The list is Empty
```

This example shows how to display the MCL failures:

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----------------------

The list is Empty
```

This example shows how to display the PRC failures:

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----------------------

 The list is Empty
```

show switch

To display information that is related to the stack member or the switch stack, use the **show switch** command in EXEC mode.

show switch [*stack-member-number*| **detail**| **neighbors**| **stack-ports** [**summary**]]

Syntax Description

stack-member-number	(Optional) Number of the stack member. The range is 1 to 9.
detail	(Optional) Displays detailed information about the stack ring.
neighbors	(Optional) Displays the neighbors of the entire switch stack.
stack-ports	(Optional) Displays port information for the entire switch stack.
summary	(Optional) Displays the stack cable length, the stack link status, and the loopback status.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command displays these states:

- Initializing—A switch has been just added to the stack and it has not completed the basic initialization to go to the ready state.
- HA Sync in Progress—After the standby is elected, the corresponding switch remains in this state until the synchronization is completed.
- Syncing—A switch that is added to an already existing stack remains in this state until the switch add sequence is complete.
- Ready—The member has completed loading the system- and interface-level configurations and can forward traffic.
- V-Mismatch—A switch in version mismatch mode. Version-mismatch mode is when a switch that joins the stack has a software version that is incompatible with the active switch.
- Provisioned—The state of a preconfigured switch before it becomes an active member of a switch stack. The MAC address and the priority number in the display are always 0 for the provisioned switch.
- Unprovisioned—The state of a switch when the provisioned switch number was unprovisioned using the **no switch** *switch-number* **provision** command.
- Removed—A switch that was present in the stack was removed using the **reload slot** command.
- Sync not started—When multiple switches are added to an existing stack together, the active switch adds them one by one. The switch that is being added is in the Syncing state. The switches that have not been added yet are in the Sync not started state.
- Lic-Mismatch—A switch has a different license level than the active switch.

A typical state transition for a stack member (including an active switch) booting up is Waiting > Initializing > Ready.

A typical state transition for a stack member in version mismatch (VM) mode is Waiting > Ver Mismatch.

You can use the **show switch** command to identify whether the provisioned switch exists in the switch stack. The **show running-config** and the **show startup-config** privileged EXEC commands do not provide this information.

The display also includes stack MAC-persistency wait-time if persistent MAC address is enabled.

This example shows how to display summary stack information:

```
Device# show switch
Switch/Stack Mac Address : 6400.f124.e900
                                           H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------
 1       Member   0000.0000.0000     0      0       Provisioned
 2       Member   0000.0000.0000     0      0       Removed
*3       Active   6400.f124.e900     2      0       Ready
```

```
 8       Member   0000.0000.0000     0      0       Unprovisioned
```

This example shows how to display detailed stack information:

```
Device# show switch detail
Switch/Stack Mac Address : 2037.06ce.3f80 - Local Mac Address
Mac persistency wait time: Indefinite
                                            H/W   Current
Switch#   Role   Mac Address     Priority Version  State
-----------------------------------------------------------
*1       Active 2037.06ce.3f80     1      0       Ready
 2       Member 0000.000.0000      0      0       Provisioned
 6       Member 2037.06ce.1e00     1      0       Ready

           Stack Port Status             Neighbors
Switch#   Port 1     Port 2           Port 1   Port 2
-----------------------------------------------------------
  1       Ok         Down              6        None
  6       Down       Ok               None       1
```

This example shows how to display the member 6 summary information:

```
Device# show switch 6
Switch#  Role      Mac Address     Priority     State
-----------------------------------------------------------
 6       Member     0003.e31a.1e00     1         Ready
```

This example shows how to display the neighbor information for a stack:

```
Device# show switch neighbors
  Switch #    Port A       Port B
  --------    ------       ------
      6        None           8
      8         6            None
```

This example shows how to display stack-port information:

```
Device# show switch stack-ports
  Switch #    Port A       Port B
  --------    ------       ------
    6          Down          Ok
    8           Ok          Down
```

This example shows the output for the **show switch stack-ports summary** command. The table that follows describes the fields in the display.

```
Device# show switch stack-ports summary
Switch#/  Stack   Neighbor   Cable    Link   Link   Sync      #         In
 Port#     Port               Length    OK   Active   OK    Changes   Loopback
          Status                                        To LinkOK
--------  ------  --------  --------  ----  ------  ----  ---------  --------
  1/1     Down      2       50 cm     No     NO      No      10         No
  1/2     Ok        3       1 m       Yes    Yes     Yes     0          No
  2/1     Ok        5       3 m       Yes    Yes     Yes     0          No
  2/2     Down      1       50 cm     No     No      No      10         No
  3/1     Ok        1       1 m       Yes    Yes     Yes     0          No
  3/2     Ok        5       1 m       Yes    Yes     Yes     0          No
  5/1     Ok        3       1 m       Yes    Yes     Yes     0          No
  5/2     Ok        2       3 m       Yes    Yes     Yes     0          No
```

Table 32: Show switch stack-ports summary Command Output

Field	Description
Switch#/Port#	Member number and its stack port number.

Field	Description
Stack Port Status	Status of the stack port. • Absent—No cable is detected on the stack port. • Down—A cable is detected, but either no connected neighbor is up, or the stack port is disabled. • OK—A cable is detected, and the connected neighbor is up.
Neighbor	Switch number of the active member at the other end of the stack cable.
Cable Length	Valid lengths are 50 cm, 1 m, or 3 m. If the switch cannot detect the cable length, the value is *no cable*. The cable might not be connected, or the link might be unreliable.
Link OK	Whether the stack cable is connected and functional. There may or may not be a neighbor connected on the other end. The *link partner* is a stack port on a neighbor switch. • No—There is no stack cable connected to this port or the stack cable is not functional. • Yes—There is a functional stack cable connected to this port.
Link Active	Whether a neighbor is connected on the other end of the stack cable. • No—No neighbor is detected on the other end. The port cannot send traffic over this link. • Yes—A neighbor is detected on the other end. The port can send traffic over this link.
Sync OK	Whether the link partner sends valid protocol messages to the stack port. • No—The link partner does not send valid protocol messages to the stack port. • Yes—The link partner sends valid protocol messages to the port.

Field	Description
# Changes to LinkOK	The relative stability of the link. If a large number of changes occur in a short period of time, link flapping can occur.
In Loopback	Whether a stack cable is attached to a stack port on the member. • No— At least one stack port on the member has an attached stack cable. • Yes—None of the stack ports on the member has an attached stack cable.

show trace messages capwap ap ha

To display wireless control and provisioning of wireless access points (CAPWAP) high availability, use the **show trace messages capwap ap ha** privileged EXEC command.

show trace messages capwap ap ha [**detail**| **event**| **dump**] [**switch** *switch*]

Syntax Description

detail	(Optional) Displays wireless CAPWAP high availability details.
detail*switch number*	Specifies the device number. Value is one.
event	(Optional) Displays wireless CAPWAP high availability events.
event*switch number*	Specifies the device number. Value is one.
dump	(Optional) Displays wireless CAPWAP high availability output.
dump *switch number*	Specifies the device number. Value is one.
switch	(Optional) Displays the device number. The value is one.
switch *switch number*	Specifies the device number. Value is one.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display CAPWAP high availability output:

```
Device# show trace messages mobility ha dump switch 1
|  Output modifiers
  <cr>
```

show trace messages mobility ha

To display wireless mobility high availability, use the **show trace messages mobility ha** privileged EXEC command.

show trace messages mobility ha [**event**| **detail**| **dump**] [**switch** *switch*]

Syntax Description

event	(Optional) Displays wireless mobility HA events.
event *switch*	Specifies the device number. Value is one.
detail	(Optional) Displays wireless mobility HA details.
detail *switch*	Specifies the device number. Value is one.
dump	(Optional) Displays the wireless mobility HA output debugging.
dump *switch*	Specifies the device number. Value is one.
switch *switch*	(Optional) Displays the device number.
switch *switch*	Specifies the device number. Value is one.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display wireless mobility high availability:

```
Device# show trace messages mobility ha
```

stack-mac persistent timer

To enable the persistent MAC address feature, use the **stack-mac persistent timer** command in global configuration mode on the switch stack or on a standalone switch. To disable the persistent MAC address feature, use the **no** form of this command.

stack-mac persistent timer [**0**| *time-value*]

no stack-mac persistent timer

Syntax Description

0	(Optional) Continues using the MAC address of the current active switch indefinitely, even after a new active switch takes over.
time-value	(Optional) Time period in minutes before the stack MAC address changes to that of the new active switch. The range is 1 to 60 minutes.

Command Default

Persistent MAC address is disabled. The MAC address of the stack is always that of the first active switch.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the stack MAC address will always be the MAC address of the first active switch, even if a new active switch takes over. The same behavior occurs when you enter the **stack-mac persistent timer** command or the **stack-mac persistent timer 0** command.

When you enter the **stack-mac persistent timer** command with a *time-value*, the stack MAC address will change to that of the new active switch after the period of time that you entered whenever a new switch becomes the active switch. If the previous active switch rejoins the stack during that time period, the stack retains its MAC address for as long as the switch that has that MAC address is in the stack.

If the whole stack reloads the MAC address of the active switch is the stack MAC address.

Note If you do not change the stack MAC address, Layer 3 interface flapping does not occur. This also means that a foreign MAC address (a MAC address that does not belong to any of the switches in the stack) could be the stack MAC address. If the switch with this foreign MAC address joins another stack as the active switch, two stacks will have the same stack MAC address. You must use the **stack-mac update force** command to resolve the conflict.

This example shows how to enable a persistent MAC address:

```
Device(config)# stack-mac persistent timer
```

You can verify your settings by entering the **show running-config** privileged EXEC command. If enabled, **stack-mac persistent timer** is shown in the output.

stack-mac update force

To update the stack MAC address to the MAC address of the active switch, use the **stack-mac update force** command in EXEC mode on the active switch.

stack-mac update force

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

By default, the stack MAC address is not changed to the MAC address of the new active switch during a high availability (HA) failover. Use the **stack-mac update force** command to force the stack MAC address to change to the MAC address of the new active switch.

If the switch with the same MAC address as the stack MAC address is currently a member of the stack, the **stack-mac update force** command has no effect. (It does not change the stack MAC address to the MAC address of the active switch.)

Note If you do not change the stack MAC address, Layer 3 interface flapping does not occur. It also means that a foreign MAC address (a MAC address that does not belong to any of the switches in the stack) could be the stack MAC address. If the switch with this foreign MAC address joins another stack as the active switch, two stacks will have the same stack MAC address. You must use the **stack-mac update force** command to resolve the conflict.

This example shows how to update the stack MAC address to the MAC address of the active switch:

```
Device> stack-mac update force
Device>
```

You can verify your settings by entering the **show switch** privileged EXEC command. The stack MAC address includes whether the MAC address is local or foreign.

standby console enable

To enable access to the standby console switch, use the **standby console enable** command in redundancy main configuration submode. To disable access to the standby console switch, use the **no** form of this command.

standby console enable

no standby console enable

Syntax Description

This command has no arguments or keywords.

Command Default

Access to the standby console switch is disabled.

Command Modes

Redundancy main configuration submode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

This command is used to collect and review specific data about the standby console. The command is useful primarily for Cisco technical support representatives troubleshooting the switch.

This example shows how to enter the redundancy main configuration submode and enable access to the standby console switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)#
```

switch stack port

To disable or enable the specified stack port on the member, use the **switch** command in privileged EXEC mode on a stack member.

switch *stack-member-number* **stack port** *port-number* {**disable**| **enable**}

Syntax Description

stack-member-number	Current stack member number. The range is 1 to 9.
stack port *port-number*	Specifies the stack port on the member. The range is 1 to 2.
disable	Disables the specified port.
enable	Enables the specified port.

Command Default

The stack port is enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A stack is in the full-ring state when all members are connected through the stack ports and are in the ready state.

The stack is in the partial-ring state when the following occurs:

- All members are connected through their stack ports but some are not in the ready state.
- Some members are not connected through the stack ports.

Note Be careful when using the **switch** *stack-member-number* **stack port** *port-number* **disable** command. When you disable the stack port, the stack operates at half bandwidth.

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the full-ring state, you can disable only one stack port. This message appears:

```
Enabling/disabling a stack port may cause undesired stack changes. Continue?[confirm]
```

If you enter the **switch** *stack-member-number* **stack port** *port-number* **disable** privileged EXEC command and the stack is in the partial-ring state, you cannot disable the port. This message appears:

```
Disabling stack port not allowed with current stack configuration.
```

This example shows how to disable stack port 2 on member 4:

```
Device# switch 4 stack port 2 disable
```

switch priority

To change the stack member priority value, use the **switch priority** command in EXEC mode on the active switch.

switch *stack-member-number* **priority** *new-priority-value*

Syntax Description

stack-member-number	Current stack member number. The range is 1 to 9.
new-priority-value	New stack member priority value. The range is 1 to 15.

Command Default

The default priority value is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The new priority value is a factor when a new active switch is elected. When you change the priority value the active switch is not changed immediately.

This example shows how to change the priority value of stack member 6 to 8:

```
Device# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

To supply a configuration to a new switch before it joins the switch stack, use the **switch provision** command in global configuration mode on the active switch. To delete all configuration information that is associated with the removed switch (a stack member that has left the stack), use the **no** form of this command.

switch *stack-member-number* **provision** *type*

no switch *stack-member-number* **provision**

Syntax Description

stack-member-number	Stack member number. The range is 1 to 9.
type	Switch type of the new switch before it joins the stack.

Command Default

The switch is not provisioned.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For *type*, enter the model number of a supported switch that is listed in the command-line help strings.

To avoid receiving an error message, you must remove the specified switch from the switch stack before using the **no** form of this command to delete a provisioned configuration.

To change the switch type, you must also remove the specified switch from the switch stack. You can change the stack member number of a provisioned switch that is physically present in the switch stack if you do not also change the switch type.

If the switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack, the switch stack applies the default configuration to the provisioned switch and adds it to the stack. The switch stack displays a message when it applies the default configuration.

Provisioned information appears in the running configuration of the switch stack. When you enter the **copy running-config startup-config** privileged EXEC command, the provisioned configuration is saved in the startup configuration file of the switch stack.

Caution When you use the **switch provision** command, memory is allocated for the provisioned configuration. When a new switch type is configured, the previously allocated memory is not fully released. Therefore, do not use this command more than approximately 200 times, or the switch will run out of memory and unexpected behavior will result.

This example shows how to provision a switch with a stack member number of 2 for the switch stack. The **show running-config** command output shows the interfaces associated with the provisioned switch.

```
Device(config)# switch 2 provision WS-xxxx
Device(config)# end
Device# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
```

```
interface GigabitEthernet2/0/3
<output truncated>
```

You also can enter the **show switch** user EXEC command to display the provisioning status of the switch stack.

This example shows how to delete all configuration information about stack member 5 when the switch is removed from the stack:

```
Device(config)# no switch 5 provision
```

You can verify that the provisioned switch is added to or removed from the running configuration by entering the **show running-config** privileged EXEC command.

switch renumber

To change the stack member number, use the **switch renumber** command in EXEC mode on the active switch.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number	Current stack member number. The range is 1 to 9.
new-stack-member-number	New stack member number for the stack member. The range is 1 to 9.

Command Default

The default stack member number is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If another stack member is already using the member number that you just specified, the active switch assigns the lowest available number when you reload the stack member.

Note If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

This example shows how to change the member number of stack member 6 to 7:

```
Device# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
 configuration.
Do you want to continue?[confirm]
```

PART XIV

System Management

- System Management Commands, page 809
- Tracing Commands, page 911

CHAPTER 15

System Management Commands

- arp, page 812
- boot, page 812
- cat, page 813
- clear location, page 814
- clear location statistics, page 815
- clear nmsp statistics, page 816
- clear wireless ccx statistics, page 816
- clear wireless client tsm dot11, page 817
- clear wireless location s69 statistics, page 818
- copy, page 818
- copy startup-config tftp:, page 819
- copy tftp: startup-config, page 820
- debug call-admission wireless all, page 821
- debug rfid, page 821
- debug voice diagnostics mac-address, page 822
- debug wps mfp, page 823
- delete, page 824
- dir, page 825
- emergency-install, page 826
- exit, page 828
- flash_init, page 828
- help, page 829
- license right-to-use, page 830
- location, page 831

- location algorithm, page 835
- location expiry, page 835
- location notify-threshold, page 836
- location plm calibrating, page 837
- location rfid, page 838
- location rssi-half-life, page 839
- mac address-table move update, page 840
- mgmt_init, page 841
- mkdir, page 842
- more, page 842
- nmsp notification interval, page 843
- no debug all, page 844
- rename, page 845
- reset, page 846
- rmdir, page 847
- sdm prefer, page 847
- set, page 848
- show avc client, page 851
- show avc wlan, page 851
- show cable-diagnostics tdr, page 852
- show debug, page 855
- show env, page 856
- show env xps, page 857
- show flow monitor, page 861
- show license right-to-use, page 865
- show location, page 867
- show location ap-detect, page 868
- show mac address-table move update, page 869
- show nmsp, page 870
- show sdm prefer, page 871
- show tech-support wireless, page 872
- show wireless band-select, page 874
- show wireless client calls, page 875

- show wireless client dot11, page 876
- show wireless client location-calibration, page 876
- show wireless client probing, page 877
- show wireless client summary, page 878
- show wireless client timers, page 878
- show wireless client voice diagnostics, page 879
- show wireless country, page 880
- show wireless detail, page 883
- show wireless dtls connections, page 883
- show wireless flow-control, page 884
- show wireless flow-control statistics, page 885
- show wireless load-balancing, page 886
- show wireless performance, page 886
- show wireless pmk-cache, page 887
- show wireless probe, page 888
- show wireless sip preferred-call-no, page 888
- show wireless summary, page 889
- shutdown, page 890
- system env temperature threshold yellow, page 891
- test cable-diagnostics tdr, page 892
- traceroute mac, page 893
- traceroute mac ip, page 895
- trapflags, page 897
- trapflags client, page 898
- type, page 899
- unset, page 900
- version, page 901
- wireless client, page 902
- wireless client mac-address deauthenticate, page 903
- wireless client mac-address, page 904
- wireless load-balancing, page 909
- wireless sip preferred-call-no, page 910

arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Shows the ARP table or the mapping for a specific IP address.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The ARP table contains the IP-address-to-MAC-address mappings.

Example

This example shows how to display the ARP table:

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

boot [**-post** | **-n** | **-p** |*flag*] *filesystem:/file-url...*

Syntax Description

-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pause for the Cisco IOS Debugger immediately after launching.

-p	(Optional) Pause for the JTAG Debugger right after loading the image.
filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url	Path (directory) and name of a bootable image. Separate image names with a semicolon.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the device attempts to automatically boot the system by using the information in the BOOT environment variable, if any.

If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you specify boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session.

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

After entering this command, you are prompted to start the setup program.

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem:	Specifies a file system.

/file-url	Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Example

This example shows how to display the contents of an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear location

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags information in the entire database, use the **clear location** command in EXEC mode.

clear location [mac-address *mac-address* | **rfid]**

Syntax Description

mac-address *mac-address*	MAC address of a specific RFID tag.
rfid	Specifies all of the RFID tags in the database.

Command Default No default behavior or values.

Command Modes User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to clear information about all of the RFID tags in the database:

```
Device> clear location rfid
```

clear location statistics

To clear radio-frequency identification (RFID) statistics, use the **clear location statistics** command in EXEC mode.

clear location statistics

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **clear location rfid** command and shows how to clear RFID statistics:

```
Device> clear location statistics
```

clear nmsp statistics

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

clear nmsp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User Exec

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **clear nmsp statistics** command and shows how to clear all statistics about NMSP information exchanged between the controller and the connected Cisco Mobility Services Engine (MSE):

```
Device> clear nmsp statistics
```

clear wireless ccx statistics

To clear CCX statistics, use the **clear wireless ccx statistics** command in EXEC mode.

clear wireless ccx statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **clear wireless ccx statistics** command and shows how to clear all collected statistics about CCX clients:

```
Device> clear wireless ccx statistics
```

clear wireless client tsm dot11

To clear the traffic stream metrics (TSM) statistics for a particular access point or all of the access points to which this client is associated, use the **clear wireless client tsm dot11** command in EXEC mode.

clear wireless client tsm dot11 {**24ghz**| **5ghz**} *client-mac-addr* {**all**| **name** *ap-name*}

Syntax Description

24ghz	Specifies the 802.11a network.
5ghz	Specifies the 802.11b network.
client-mac-addr	MAC address of the client.
all	Specifies all access points.
name *ap-name*	Name of a Cisco lightweight access point.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **clear wireless client tsm dot11** command and shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98 on all of the access points 5-GHz radios where this client is known:

```
Device> clear wireless client tsm dot11 5ghz 00:40:96:a8:f7:98 all
```

clear wireless location s69 statistics

To clear statistics about S69 exchanges with CCXv5 clients, use the **clear wireless location s69 statistics** command in EXEC mode.

clear wireless location s69 statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

S69 messages are exchanged between CCXv5 clients and the wireless infrastructure. The CCXv5 client uses S69 message to request location information, that is then returned by the wireless infrastructure through a S69 response message.

Example

The following is sample output from the **clear wireless location s69 statistics** command and shows how to clear statistics about S69 exchanges with CCXv5 clients:

```
Device> clear wireless location s69 statistics
```

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Path (directory) and filename (source) to be copied.
/destination-file-url	Path (directory) and filename of the destination.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Example

This example shows how to copy a file at the root:

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

copy startup-config tftp: *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

To copy your current configurations from the switch, run the command **copy startup-config tftp:** and follow the instructions. The configurations are copied onto the TFTP server.

Then, login to another switch and run the command **copy tftp: startup-config** and follow the instructions. The configurations are now copied onto the other switch.

Example

This example shows how to copy the configuration settings onto a TFTP server:

```
Device: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

copy tftp: startup-config *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

After the configurations are copied, to save your configurations, use **write memory** command and then either reload the switch or run the **copy startup-config running-config** command.

Example

This example shows how to copy the configuration settings from the TFTP server onto a switch:

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

debug call-admission wireless all

To enable debugging of the wireless Call Admission Control (CAC) feature, use the **debug call-admission wireless all** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug call-admission wireless all [**switch** *switch*]

no debug call-admission wireless all [**switch** *switch*]

Syntax Description

switch	Configures debugging options for all wireless CAC messages associated to a particular switch.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **debug call-admission wireless switch** command and shows how to enable debugging options for CAC messages:

```
Device# debug call-admission wireless switch 1 all
```

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug rfid {*debug_leaf_name*| **all** | **detail** |**error**|**nmsp**|**receive**}[**filter**|**switch** *switch*]

no debug rfid {*debug_leaf_name*| **all** | **detail** | **error** | **nmsp** | **receive**}[**filter** | **switch** *switch*]

Syntax Description

debug_leaf_name	Debug leaf name.
all	Configures debugging of all RFID.
detail	Configures debugging of RFID detail.
error	Configures debugging of RFID error messages.
nmsp	Configures debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures debugging of incoming RFID tag messages.
filter	Debug flag filter name.
switch *switch*	Configures RFID debugging for device.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **debug rfid** command and shows how to enable debugging of RFID error messages:

```
Device# debug rfid error switch 1
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

Syntax Description

voice diagnostics	Configures voice debugging for voice clients.

mac-address *mac-address1* **mac-address** *mac-address2*	Specifies MAC addresses of the voice clients.
verbose	Enables verbose mode for voice diagnostics.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug wps mfp

To enable WPS MFP debugging options, use the **debug wps mfp** command in privileged EXEC mode. To disable debugging, use the no form of this command.

debug wps mfp {**all** | **capwap**| **client** | **detail**| **mm**| **report**}[**switch** *switch*]

Syntax Description

wps mfp	Configures WPS MFP debugging options.
all	Displays all WPS MFP debugging messages.
capwap	Displays MFP messages.
client	Displays client MFP messages.
detail	Displays detailed MFP CAPWAP messages.
mm	Displays MFP mobility (inter-controller) messages.
report	Displays MFP reports.
switch *switch*	Displays the WPS MFP debugging for the device.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable WPS MFP debugging options for client:

```
Device# debug wps mfp client switch 1
```

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/file-url...	Path (directory) and filename to delete. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

Example

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0:** boot loader command.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url	(Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot Loader

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Example

This example shows how to display the files in flash memory:

```
Device: dir flash:
Directory of flash:/
    2  -rwx        561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx    2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx       1048   Mar 01 2013 00:01:39  multiple-fs
```

```
  6  drwx        512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx        512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx       4316   Mar 01 2013 01:14:05  config.text
648 -rwx          5   Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

Table 33: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

emergency-install

To perform an emergency installation on your system, use the **emergency-install** command in boot loader mode.

emergency-install *url://<url>*

Syntax Description

<url>	URL and name of the file containing the emergency installation bundle image.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The boot flash is erased during the installation operation.

Example

This example shows how to perform the emergency install operation using the contents of an image file:

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range          \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)



Initiating Emergency Installation of bundle                                          \
tftp:<url>


Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                        \
+++@@@@####...++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!

Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
```

```
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

    boot
```

exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to exit the configuration mode:

```
Device(config)# exit
Device#
```

flash_init

To initialize the flash: file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Command Default

The flash: file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

During the normal boot process, the flash: file system is automatically initialized.

Use this command to manually initialize the flash: file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
```

```
unset -- Unset one or more environment variables
version -- Display boot loader version
```

license right-to-use

To configure right-to-use access point adder licenses on the device, use the **license right-to-use** command in privileged EXEC mode.

license right-to-use {**activate | deactivate**} **apcount | ipbase | ipservices | lanbase**

Syntax Description

activate	Activates permanent or evaluation ap-count licenses.
deactivate	Deactivates permanent or evaluation ap-count licenses.
apcount *count*	Specifies the number of ap-count licenses added. You can configure the number of adder licenses from 5 to 50.
ipbase *count*	Activates ipbase licenses on the switch.
ipservices *count*	Activates ipservices licenses on the switch.
lanbase *count*	Activates lanbase licenses on the switch.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to activate an ap-count evaluation license:

```
Device# license right-to-use activate apcount evaluation
Device# end
```

This example shows how to activate an ap-count permanent license:

```
Device# license right-to-use deactivate apcount evaluation
Device# end
```

This example shows how to add a new ap-count license:

```
Device# license right-to-use activate apcount 500 slot 1
Device# end
```

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}| **expiry**{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}| **geo-location identifier** {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status** |**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** { **calibrating-client***seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

no location {**admin-tag** *string*| **algorithm**| **civic-location identifier** {**host**| *id*}| **civic-location identifier** {**host**| *id*}| **elin-location** {*string* |**identifier** *id*}| **expiry**{**calibrating-client***timeout-value*|**client***timeout-value*|**rouge-aps***timeout-value*|**tags***timeout-value*}| **geo-location identifier** {**host**| *id*}| **notify-threshold**{**client***db*|**rouge-aps***db*|**tags***db*| **plm**{**calibrating**| {**multiband | uniband**}| **client***burst-interval*}| **prefer**{**cdp weight***priority-value*|**lldp-med weight***priority-value*|**static config weight***priority-value*}|**rfid**{**status** |**timeout***rfid-timeout-value*|**vendor-name***name*}|**rssi-half-life** { **calibrating-client***seconds*|**client***seconds*|**rogue-aps***seconds*|**tags***seconds*}

Syntax Description

admin-tag*string*	Configures administrative tag or site information. Site or location information in alphanumeric format.
algorithm	Configures the algorithm used to average RSSI and SNR values.
civic-location	Configures civic location information.
identifier	Specifies the name of the civic location, emergency, or geographical location.

host	Defines the host civic or geo-spatial location.
id	Name of the civic, emergency, or geographical location. **Note** The identifier for the civic location in the LLDP-MED switch TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
elin-location	Configures emergency location information (ELIN).
expiry {calibrating-client | client | rogue-aps | tags} *timeout-value*	Configures the timeout for RSSI values for calibrating clients, clients, rouge access points, and RFID tags. The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds. The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds
geo-location	Configures geo-spatial location information.
notify-threshold {client| rogue-aps| tags} *db*	Configures the NMSP notification threshold for RSSI measurements. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
calibrating {multiband | uniband} | client *seconds*	Configures path loss measurement (CCX S60) request for calibrating clients and burst interval for clients. The valid range for the burst interval parameter is 0 to 3600 seconds.
prefer	Sets location information source priority.
rfid	Configures RFID tag tracking for a location.
rssi-half-life	Configures the RSSI half life for various devices.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code—**Sets an additional civic location code.
- **additional-location-information—**Sets additional civic location information.
- **branch-road-name—**Sets the branch road name.
- **building—**Sets building information.
- **city—**Sets the city name.
- **country—**Sets the two-letter ISO 3166 country code.
- **county—**Sets the county name.
- **default—**Sets a command to its defaults.
- **division—**Sets the city division name.
- **exit—**Exits from the civic location configuration mode.
- **floor—**Sets the floor number.
- **landmark—**Sets landmark information.
- **leading-street-dir—**Sets the leading street direction.
- **name—**Sets the resident name.
- **neighborhood—**Sets neighborhood information.
- **no—**Negates the specified civic location data and sets the default value.
- **number—**Sets the street number.
- **post-office-box—**Sets the post office box.
- **postal-code—**Sets the postal code.
- **postal-community-name—**Sets the postal community name.
- **primary-road-name—**Sets the primary road name.
- **road-section—**Sets the road section.
- **room—**Sets room information.
- **seat—**Sets seat information.
- **state—**Sets the state name.

- **street-group—**Sets the street group.
- **street-name-postmodifier—**Sets the street name postmodifier.
- **street-name-premodifier—**Sets the street name premodifier.
- **street-number-suffix—**Sets the street number suffix.
- **street-suffix—**Sets the street suffix.
- **sub-branch-road-name—**Sets the sub-branch road name.
- **trailing-street-suffix—**Sets the trailing street suffix.
- **type-of-place—**Sets the type of place.
- **unit—**Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude—**Sets altitude information in units of floor, meters, or feet.
- **latitude—**Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude—**Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution—**Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default—**Sets the geographical location to its default attribute.
- **exit—**Exits from geographical location configuration mode.
- **no—**Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

This example shows how to configure civic location information on the switch:

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name “Cisco Way”
Device(config-civic)# city “San Jose”
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county “Santa Clara”
Device(config-civic)# country US
Device(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the switch:

```
Device(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the switch:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

location algorithm

To configure the algorithm used to average RSSI and SNR values, use the **location algorithm** command in global configuration mode. To remove the algorithm used to average RSSI and SNR values, use the **no** form of this command.

location algorithm {**rssi-average | simple**}

no location algorithm {**rssi-average | simple**}

Syntax Description

rssi-average	Specifies a more accurate algorithm but with more CPU overhead.
simple	Specifies faster algorithm with smaller CPU overhead but less accuracy.

Command Default

RSSI average

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a more accurate algorithm but with more CPU overhead:

```
Device# configure terminal
Device(config)# location algorithm rssi-average
Device(config)# end
```

location expiry

To configure the timeout for RSSI values, use the **location expiry** command in global configuration mode.

location expiry {**calibrating-client | client | rogue-aps | tags** } *timeout-value*

Syntax Description

calibrating-client	Specifies the RSSI timeout value for calibrating clients.
client	(Optional) Specifies the RSSI timeout value for clients.
rogue-aps	Specifies the RSSI timeout value for rogue access points.
tags	Specifies the RSSI timeout value for RFID tags.
timeout-value	The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds. The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the RSSI timeout value for wireless clients:

```
Device# configure terminal
Device(config)# location expiry client 1000
Device(config)# end
```

location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

location notify-threshold {**client | rogue-aps | tags** } *db*

no location notify-threshold {**client | rogue-aps | tags** }

Syntax Description

client	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
rogue-aps	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
tags	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
db	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(config)# end
```

location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command in global configuration mode.

location plm calibrating {**multiband** | **uniband**}

Syntax Description

multiband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
uniband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

location rfid

To configure RFID tag tracking for a location, use the **location rfid** command in global configuration mode. To remove a RFID tag tracking for a location, use the **no** form of this command.

location rfid { **status**| **timeout** *seconds*| **vendor-name** *name*}

no location rfid { **status**| **timeout** *seconds*| **vendor-name**}

Syntax Description

status	Enables location tracking for RFID tags. The **no location rfid status** command disables location tracking for tags.
timeout *seconds*	Specifies the location RFID timeout value. Determines the amount of time for which a detected RFID location information is considered as valid. Any RSSI change (below the RSSI threshold) in the configured interval do not result in a new location computation and a message is sent to the MSE. The valid timeout range is from 60 through 7200 seconds.
vendor-name *name*	Specifies the RFID tag vendor name.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **no location rfid status** command disables location RFID status. The **no location rfid timeout** command returns to the default timeout value. The **no location rfid vendor-name** disables tracking for a particular vendor.

The example shows how to configure the static RFID tag data timeout:

```
Device# configure terminal
Device(config)# location rfid timeout 1000
Device(config)# end
```

location rssi-half-life

To configure the RSSI half life for various devices, use the **location rssi-half-life** command in global configuration mode. To remove a RSSI half life for various devices, use the **no** form of this command.

location rssi-half-life {**calibrating-client | client | rogue-aps | tags** } *seconds*

no location rssi-half-life {**calibrating-client | client | rogue-aps | tags** }

Syntax Description

calibrating-client	Specifies the RSSI half life for calibrating clients.
client	Specifies the RSSI half life for clients.
rogue-aps	Specifies the RSSI half life for rogue access points.
tags	Specifies the RSSI half life for RFID tags.
seconds	The valid range for the half-life parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure the half life value for a client RSSI to 100 seconds:

```
Device# configure terminal
Device(config)# location rssi-half-life client 100
Device(config)# end
```

mac address-table move update

To enable the MAC address table move update feature, use the **mac address-table move update** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

mac address-table move update {**receive | transmit**}

no mac address-table move update {**receive | transmit**}

Syntax Description

receive	Specifies that the switch processes MAC address-table move update messages.
transmit	Specifies that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.

Command Default

By default, the MAC address-table move update feature is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.

You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

Examples

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update receive
Device(config)# end
```

You can verify your setting by entering the **show mac address-table move update** privileged EXEC command.

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init** command in boot loader mode.

mgmt_init

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Example

This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Name of the directories to create. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Example

This example shows how to make a directory called Saved_Configs:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Example

This example shows how to display the contents of a file:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

nmsp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmsp notification interval** command in global configuration mode.

nmsp notification interval { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

Syntax Description

attachment	Specifies the time used to aggregate attachment information.

location	Specifies the time used to aggregate location information.
rssi	Specifies the time used to aggregate RSSI information.
clients	Specifies the time interval for clients.
rfid	Specifies the time interval for rfid tags.
rogues	Specifies the time interval for rogue APs and rogue clients .
ap	Specifies the time used to aggregate rogue APs .
client	Specifies the time used to aggregate rogue clients.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(config)# end
```

no debug all

To disable debugging on a switch, use the **no debug all** command in Privileged EXEC mode.

no debug all

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Example

This example shows how to disable debugging on a switch.

```
Device: no debug all
All possible debugging has been turned off.
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Original path (directory) and filename.
/destination-file-url	New path (directory) and filename.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Example

This example shows a file named *config.text* being renamed to *config1.text*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem:* boot loader command.

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Example

This example shows how to reset the system:

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all of the files in the directory.

The device prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

sdm prefer

To specify the SDM template for use on the switch, use the **sdm prefer** command in global configuration mode.

sdm prefer {**advanced**}

Syntax Description

advanced	Supports advanced features such as NetFlow.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In a device stack, all stack members must use the same SDM template that is stored on the active device.

When a new device is added to a stack, the SDM configuration that is stored on the active device overrides the template configured on an individual device.

Example

This example shows how to configure the advanced template:

```
Device(config)# sdm prefer advanced
Device(config)# exit
Device# reload
```

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

set *variable value*

Syntax Description

variable value	Use one of the following keywords for *variable* and the appropriate value for *value*: **MANUAL_BOOT—**Decides whether the device automatically or manually boots. Valid values are 1/Yes and 0/No. If it is set to 0 or No, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the device from the boot loader mode.

BOOT *filesystem:/file-url*—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting.

If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.

ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the **Break** key on the console.

Valid values are 1, Yes, On, 0, No, and Off. If set to 1, Yes, or On, you can interrupt the automatic boot process by pressing the **Break** key on the console after the flash: file system has initialized.

HELPER *filesystem:/file-url*—Identifies a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

PS1 *prompt*—Specifies a string that is used as the command-line prompt in boot loader mode.

CONFIG_FILE flash: */file-url*—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.

BAUD *rate*—Specifies the number of bits per second (b/s) that is used for the baud rate for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 128000 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.

The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.

SWITCH_NUMBER *stack-member-number*—Changes the member number of a stack member.

SWITCH_PRIORITY *priority-number*—Changes the priority value of a stack member.

Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the **Break** key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash: file system in various files. Each line in the files contains an environment variable name and an equal sign followed by the value of the variable.

A variable has no value if it is not listed in these files; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value.

Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash: file system.

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem://file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem: / file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:** */file-url* global configuration command.

The SWITCH_NUMBER environment variable can also be set by using the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

show avc client *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

client *client-mac*	Specifies the client MAC address.
top *n* **application**	Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny          7343           449860           61              94
2    unknown         99             13631            137             3
3    dhcp            18             8752             486             2
4    http            18             3264             181             1
5    tftp            9              534              59              0
6    dns             2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
----------------------------------------------------------------------------
1    skinny          9              540              60               100
```

show avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

show avc wlan *ssid* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

wlan *ssid*	Specifies the Service Set IDentifier (SSID) for WLAN.
top *n* **application**	Specifies the number of top "N" applications.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show avc wlan** command:

```
Device# show avc wlan Lobby_WLAN top 10 application aggregate

Cumulative Stats:

No.  AppName           Packet-Count          Byte-Count          AvgPkt-Size  usage%
-----------------------------------------------------------------------------------------
1    ssl               10598677              1979525706             997          42
2    vnc               5550900               3764612847             678          14
3    http              3043131               2691327197             884          10
4    unknown           1856297               1140264956             614          4
5    video-over-http   1625019               2063335150             1269         8
6    binary-over-http  1329115               1744190344             1312         6
7    webex-meeting     1146872               540713787              471          2
8    rtp               923900                635650544              688          2
9    unknown           752341                911000213              1210         3
10   youtube           631085                706636186              1119         3

Last Interval(90 seconds) Stats:

No.  AppName          Packet-Count          Byte-Count            AvgPkt-Size  usage%
-----------------------------------------------------------------------------------------
1    vnc               687093                602731844              877          68
2    video-over-http   213272                279831588              1312         31
3    ssl               6515                  5029365                771          1
4    webex-meeting     3649                  1722663                472          0
5    http              2634                  1334355                506          0
6    unknown           1436                  99412                  69           0
7    google-services   722                   378121                 523          0
8    linkedin          655                   393263                 600          0
9    exchange          432                   167390                 387          0
10   gtalk-chat        330                   17330                  52           0
```

show cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id	Specifies the interface on which TDR is run.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.

Examples

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command on a device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
  TDR test last run on: March 01 00:04:08
  Interface  Speed  Local pair  Pair length         Remote pair   Pair status
  --------- ----- ---------- ------------------ ----------- --------------------
  Gi1/0/23   1000M  Pair A      1    +/- 1 meters   Pair A        Normal
                    Pair B      1    +/- 1 meters   Pair B        Normal
                    Pair C      1    +/- 1 meters   Pair C        Normal
                    Pair D      1    +/- 1 meters   Pair D        Normal
```

Table 34: Field Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.

Field	Description
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress.

This example shows the output from the **show interface** *interface-id* command when TDR is running:

```
Device# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
  % TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

show debug

show debug condition *Condition identifier* | *All conditions*

Syntax Description

Condition identifier	Sets the value of the condition identifier to be used. Range is between 1 and 1000.
All conditions	Shows all conditional debugging options available.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Example

This example shows the output of a **show debug** command:

```
Device# show debug condition all
```

To disable debugging, use the **no debug all** command.

show env

To display fan, temperature, and power information for the switch (standalone switch, stack master, or stack member), use the **show env** command in EXEC modes.

show env { **all** | **fan** | **power** [**all** | **switch** [*switch-number*]] | **stack** [*stack-number*] | **temperature** [**status**] }

Syntax Description

all	Displays fan, temperature and power environmental status.
fan	Displays the switch fan status.
power	Displays the power supply status.
all	(Optional) Displays the status for all power supplies.
switch *switch-number*	(Optional) Displays the power supply status for a specific switch.
stack *switch-number*	(Optional) Displays all environmental status for each switch in the stack or for a specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
temperature	Displays the switch temperature status.
status	(Optional) Displays the temperature status and threshold values.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any member switch.

Use the **show env temperature status** command to display the switch temperature states and threshold levels.

Example

This example shows how to display information about stack member 1 from the master switch:

```
Device> show env stack 1
Device 1:
Device Fan 1 is OK
Device Fan 2 is OK
Device Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Device 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

This example shows how to display temperature value, state, and threshold values:

```
Device> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

Table 35: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

show env xps

To display budgeting, configuration, power, and system power information for the Cisco eXpandable Power System (XPS) 2200, use the **show env xps** command in privileged EXEC mode.

show env xps { **budgeting** | **configuration** | **port** [**all** | *number*] | **power** | **system** | **thermal** | **upgrade** | **version** }

Syntax Description

budgeting	Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.
configuration	Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the show env xps configuration command to retrieve the non-default configuration.
port [**all** | *number*]	Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9.
power	Displays the status of the XPS power supplies.
system	Displays the XPS system status.
thermal	Displays the XPS thermal status.
upgrade	Displays the XPS upgrade status.
version	Displays the XPS version details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(55)SE1	This command was introduced.

Usage Guidelines

Use the **show env xps** privileged EXEC command to display the information for XPS 2200.

Example

This is an example of output from the show env xps budgeting command:

```
Switch#
=======


XPS 0101.0100.0000 :
=========================================================
Data                  Current    Power     Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
   223
    1543
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
```

```
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
9     1        1100 -    RPS-NB     223        070
XPS  -        -    1100  -          -
```

This is an example of output from the show env xps configuration command:

```
Switch# show env xps configuration
============================================
XPS 0101.0100.0000 :
============================================
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4
```

This is an example of output from the show env xps port all command:

```
Switch#
XPS 010



----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
----------------------------------------
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode            : -
Cable faults
<output truncated>
```

This is an example of output from the show env xps power command:

```
==============================================================================
XPS 0101.0100.0000 :
==============================================================================
Port-Supply SW PID                 Serial#     Status         Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK             SP   1100
1-A         -  -                   -           -
1-B         -  -                   -           -               SP    715
2-A         -  -                   -           -
2-B         -  -                   -           -
9-A                       100WAC    LIT141307RK OK              RPS  1100
9-B                    esent
```

This is an example of output from the show env xps system command:

```
Switch#
=======


XPS 0101.0100.0000 :
==============================================================================
```

```
XPS                        Cfg  Cfg      RPS Switch  Current    Data Port  XPS Port Name

Mode Role    Pri Conn    Role-State  Switch #
----  --------------------  ---- -------  --- ------  ----------  --------
1     -                    On   Auto-SP  1   Yes     SP-PS      -
2     -                    On   Auto-SP  2   Yes     SP-PS      -
3     -                    On   Auto-SP  3   No      -          -
4     none                 On   Auto-SP  5   No      -          -
5     -                    Off  Auto-SP  6   No      -          -
6     -                    On   Auto-SP  7   No      -          -
7     -                    On   Auto-SP  8   No      -          -
8     -                    On   Auto-SP  9   No      -
9     test                 On   Auto-SP  4   Yes     RPS-NB
```

This is an example of output from the show env xps thermal command:

```
Switch#
=======



XPS 0101.0100.0000 :
=============================================
Fan  Status
----  -----------
1     OK
2     OK
3     NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK
```

This is an example of output from the show env xps upgrade command when no upgrade is occurring:

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

These are examples of output from the show env xps upgrade command when an upgrade is in process:

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

This is an example of output from the show env xps version command:

```
Switch# show env xps version
=============================================
XPS 0022.bdd7.9b14:
=============================================
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18
```

Table 36: Related Commands

Command	Description
power xps(global configuration command)	Configures XPS and XPS port names.
power xps(privileged EXEC command)	Configures the XPS ports and system.

show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

show flow monitor [**broker** [**detail**| **picture**]| [**name**] *monitor-name* [**cache** [**format** {**csv**| **record**| **table**}]]| **provisioning**| **statistics**]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the flow monitor
detail	(Optional) Displays detailed information about the flow monitor broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
provisioning	(Optional) Displays the flow monitor provisioning information.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that Flexible NetFlow uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which Flexible NetFlow collects values as additional data for the cache.

The following example displays the status for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 37: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.

Field	Description
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

```
Device# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001:DB8::1
IPV6 DESTINATION ADDRESS:                2001:DB8:1::1
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

This table describes the significant fields shown in the display.

Table 38: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
Flows added	Flows added to the cache since the cache was created.

Field	Description
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
DATALINK MAC SOURCE ADDRESS INPUT	MAC source address of input packets.
DATALINK MAC DESTINATION ADDRESS INPUT	MAC destination address of input packets.
IPV6 SOURCE ADDRESS	IPv6 source address.
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

```
Device# show flow monitor FLOW-MONITOR-1 cache format table
  Cache type:                           Normal (Platform cache)
  Cache size:                          Unknown
  Current entries:                           1

  Flows added:                               3
  Flows aged:                                2
    - Active timeout      (   300 secs)      2

DATALINK MAC SRC ADDR INPUT  DATALINK MAC DST ADDR INPUT  IPV6 SRC ADDR  IPV6 DST ADDR
TRNS SRC PORT  TRNS DST PORT  IP VERSION  IP PROT  IP TOS  IP TTL  tcp flags  bytes long
pkts long
===========================  ===========================  =============  =============
=============  =============  ==========  =======  ======  ======  =========  ==========
=========
0000.0000.1000               6400.F125.59E6               2001:DB8::1    2001:DB8:1::1
```

```
       1111           2222           6        6  0x05        11  0x20        132059538
1158417
```

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

```
Device# show flow monitor name FLOW-MONITOR-IPv6 cache format record
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2

DATALINK MAC SOURCE ADDRESS INPUT:       0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                     2001::2
IPV6 DESTINATION ADDRESS:                2002::2
TRNS SOURCE PORT:                        1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                              6
IP PROTOCOL:                             6
IP TOS:                                  0x05
IP TTL:                                  11
tcp flags:                               0x20
counter bytes long:                      132059538
counter packets long:                    1158417
```

The following example displays the status and statistics for a flow monitor:

```
Device# show flow monitor FLOW-MONITOR-1 statistics
  Cache type:                               Normal (Platform cache)
  Cache size:                              Unknown
  Current entries:                               1

  Flows added:                                   3
  Flows aged:                                    2
    - Active timeout      (   300 secs)          2
```

show license right-to-use

To display detailed information for apcount adder licenses installed on the device, use the **show license right-to-use** command in EXEC modes.

show license right-to-use {**default** | **detail** | **eula** | **mismatch** | **slot** | **summary** | **usage**}

Syntax Description

default	Displays the default license information.
detail	Displays details of all the licenses in the stack.
eula	Displays the EULA text.
mismatch	Displays mismatch license information.
slot	Specifies the switch number.
summary	Displays consolidated stack-wide license information.

usage	Displays the usage details of all licenses.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show license right-to-use usage** command and displays all the detailed information:

```
Device# show license right-to-use usage

 Slot#  License Name     Type     usage-duration(y:m:d)  In-Use  EULA
-----------------------------------------------------------------------
 1      ipservices     permanent    0 :0 :1                yes   yes
 1      ipbase         permanent    0 :0 :0                no    no
 1      ipbase         evaluation   0 :0 :0                no    no
 1      lanbase        permanent    0 :0 :7                no    yes
 1      apcount        evaluation   0 :0 :0                no    no
 1      apcount        base         0 :0 :0                no    no
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes

Device#
```

The following is sample output from the **show license right-to-use detail** command and displays the detailed information of licenses:

```
Device# show license right-to-use detail

Index 1:  License Name: apcount
           Period left: 16
           License Type: evaluation
           License State: Not Activated
           License Count: 1000
           License Location: Slot 1
Index 2:  License Name: apcount
           Period left: Lifetime
           License Type: adder
           License State: Active, In use
           License Count: 125
           License Location: Slot 1
```

The following is sample output from the **show license right-to-use summary** command when the evaluation license is active:

```
Device# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
  apcount      evaluation  1000     50

-------------------------------------------

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900
```

The following is sample output from the **show license right-to-use summary** command when the adder licenses are active:

```
Device# show license right-to-use summary
  License Name    Type     Count   Period left
-----------------------------------------------
apcount      adder       125      Lifetime

-------------------------------------------

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25
```

show location

To display location information, use the **show location** command in privileged EXEC mode.

show location {**detail** *mac-addr*| **plm**| **statistics**| **summary rfid**| **rfid** {**client**| **config**| **detail** *MAC-addr*| **summary**}}

Syntax Description

detail *mac-addr*	Displays detailed location information with the RSSI table for a particular client.
plm	Displays location path loss measurement (CCX S60) configuration.
statistics	Displays location-based system statistics.
summary	Displays location-based system summary information.
rfid	Displays the RFID tag tracking information.
client	Displays the summary of RFID tags that are clients.
config	Displays the configuration options for RFID tag tracking.
detail *MAC-addr*	Displays the detailed information for one rfid tag.

summary	Displays summary information for all known rfid tags.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show location plm** command:

```
Device# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```

show location ap-detect

To display the location information detected by specified access point, use the **show location ap-detect** command in privileged EXEC mode.

show location ap-detect {**all**| **client**| **rfid**| **rogue-ap**| **rogue-client**} *ap-name*

Syntax Description

all	Displays information of the client, RFID, rogue access point, and rogue client.
client	Displays the client information.
rfid	Displays RFID information.
rogue-ap	Displays rogue access point information.
rogue-client	Displays rogue client information.
ap-name	Specified access point name.

Command Default

No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show location ap-detect client** command:

```
Device# show location ap-detect client AP02
Clients

MAC Address       Status            Slot  Antenna     RSSI
-----------------------------------------------------------
2477.0389.96ac    Associated           1        0      -60
2477.0389.96ac    Associated           1        1      -61
2477.0389.96ac    Associated           0        0      -46
2477.0389.96ac    Associated           0        1      -41


RFID Tags



Rogue AP's



Rogue Clients

MAC Address         State               Slot     Rssi
-------------------------------------------------------
0040.96b3.bce6      Alert               1        -58
586d.8ff0.891a      Alert               1        -72
```

show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show nmsp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmsp** command.

show nmsp {**attachment** | {**suppress interfaces**}| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription detail** [*ip-addr*]| **summary**}

Syntax Description

attachment suppress interfaces	Displays attachment suppress interfaces.
capability	Displays NMSP capabilities.
notification interval	Displays the NMSP notification interval.
statistics connection	Displays all connection-specific counters.
statistics summary	Displays the NMSP counters.
status	Displays status of active NMSP connections.

subscription detail *ip-addr*	The details are only for the NMSP services subscribed to by a specific IP address.
subscription summary	Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show nmsp notification interval** command:

```
Device#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 Rogue AP             : 2 sec
 Rogue Client         : 2 sec
Attachment Interval   : 30 sec
Location Interval     : 30 sec
```

show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

show sdm prefer [**advanced**]

Syntax Description

advanced	(Optional) Displays information on the advanced template.

Command Default

No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

Example

The following is sample output from the **show sdm prefer** command:

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                                4094
 Unicast MAC addresses:                          32768
 Overflow Unicast MAC addresses:                 512
 IGMP and Multicast groups:                      8192
 Overflow IGMP and Multicast groups:             512
 Directly connected routes:                      32768
 Indirect routes:                                7680
 Security Access Control Entries:                3072
 QoS Access Control Entries:                     3072
 Policy Based Routing ACEs:                      1024
 Netflow ACEs:                                   1024
 Input Microflow policer ACEs:                   256
 Output Microflow policer ACEs:                  256
 Flow SPAN ACEs:                                 256
 Tunnels:                                        256
 Control Plane Entries:                          512
 Input Netflow flows:                            8192
 Output Netflow flows:                          16384
 SGT/DGT entries:                                4096
 SGT/DGT Overflow entries:                       512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
```

show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

show tech-support wireless

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show tech-support wireless** command:

```
Device# show tech-support wireless
 *** show ap capwap timers ***

Cisco AP CAPWAP timers

AP Discovery timer       : 10
AP Heart Beat timeout    : 30
Primary Discovery timer  : 120
Primed Join timeout      : 0
Fast Heartbeat           : Disabled
Fast Heartbeat timeout   : 1
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5

AP Name                          Retransmit Interval             Retransmit Count
-----------------------------------------------------------------------------------------------
TSIM_AP-2                        3                               5
TSIM_AP-3                        3                               5
*** show ap dot11 24ghz cleanair air-quality summary ***

AQ = Air Quality
DFS = Dynamic Frequency Selection

*** show ap dot11 24ghz cleanair air-quality worst ***

AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name             Channel   Avg AQ  Min AQ  Interferers  DFS
-----------------------------------------------------------------
                    0         0       0       0            No
*** show ap dot11 24ghz cleanair config ***

Clean Air Solution................................ : Disabled
Air Quality Settings:
    Air Quality Reporting......................... : Disabled
    Air Quality Reporting Period (min)............ : 15
    Air Quality Alarms............................ : Enabled
    Air Quality Alarm Threshold................... : 10
Interference Device Settings:
    Interference Device Reporting................. : Enabled
        Bluetooth Link............................ : Enabled
        Microwave Oven............................ : Enabled
        802.11 FH................................. : Enabled
        Bluetooth Discovery....................... : Enabled
        TDD Transmitter........................... : Enabled
```

```
        Jammer..................................... : Enabled
        Continuous Transmitter..................... : Enabled
        DECT-like Phone............................ : Enabled
        Video Camera............................... : Enabled
        802.15.4................................... : Enabled
        WiFi Inverted.............................. : Enabled
        WiFi Invalid Channel....................... : Enabled
        SuperAG.................................... : Enabled
        Canopy..................................... : Enabled
        Microsoft Device........................... : Enabled
        WiMax Mobile............................... : Enabled
        WiMax Fixed................................ : Enabled
    Interference Device Types Triggering Alarms:
        Bluetooth Link............................. : Disabled
        Microwave Oven............................. : Disabled
        802.11 FH.................................. : Disabled
        Bluetooth Discovery........................ : Disabled
        TDD Transmitter............................ : Disabled
        Jammer..................................... : Disabled
        Continuous Transmitter..................... : Disabled
        DECT-like Phone............................ : Disabled
        Video Camera............................... : Disabled
  802.15.4................................... : Disabled
        WiFi Inverted.............................. : Enabled
        WiFi Invalid Channel....................... : Enabled
        SuperAG.................................... : Disabled
        Canopy..................................... : Disabled
        Microsoft Device........................... : Disabled
        WiMax Mobile............................... : Disabled
        WiMax Fixed................................ : Disabled
    Interference Device Alarms..................... : Enabled
Additional Clean Air Settings:
    CleanAir Event-driven RRM State................ : Disabled
    CleanAir Driven RRM Sensitivity................ : LOW
    CleanAir Persistent Devices state............... : Disabled
```

show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

show wireless band-select

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless band-select** command:

```
Device# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : 80
```

show wireless client calls

To display the total number of active or rejected calls on the device, use the **show wireless client calls** command in privileged EXEC mode.

show wireless client calls {**active** | **rejected**}

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client calls** command:

```
device# show wireless client calls active

TSPEC Calls:

-------------------------------------------------------------------------------
MAC Address     AP Name             Status               WLAN  Authenticated
-------------------------------------------------------------------------------
0000.1515.000f    AP-2           Associated              1  Yes

SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command in privileged EXEC mode.

show wireless client dot11 {**24ghz** | **5ghz**} **calls** {**active** | **rejected**}

Syntax Description

24ghz	Displays the 802.11b/g network.
5ghz	Displays the 802.11a network.
calls	Displays the wireless client calls.
active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client dot11** command:

```
Device# show wireless client dot11 5ghz calls active

 TSPEC Calls:
------------------


SIP Calls:
------------------
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client location-calibration

To display the list of clients currently used to perform location calibration, use the **show wireless client location-calibration** command in privileged EXEC mode.

show wireless client location-calibration

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client location-calibration** command:

```
Device# show wireless client location-calibration
```

show wireless client probing

To display the number of probing clients, use the **show wireless client probing** command in privileged EXEC mode.

show wireless client probing

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client probing** command:

```
Device# show wireless client probing
MAC Address
------------------
000b.cd15.0001
000b.cd15.0002
000b.cd15.0003
000b.cd15.0004
000b.cd15.0005
```

```
000b.cd15.0006
```

show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

show wireless client summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The following is sample output from the **show wireless client summary** command:

Use the **show wireless exclusionlist** command to display clients on the exclusion list (blacklisted).

```
Device# show wireless client summary
Number of Local Clients : 1

MAC Address    AP Name                          WLAN State              Protocol
-------------------------------------------------------------------------------
0000.1515.000f  AP-2                        1    UP                 11a
```

show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

show wireless client timers

Syntax Description

This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless client timers** command:

```
Device# show wireless client timers
 Authentication Response Timeout (seconds)      : 10
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command in privileged EXEC mode.

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rssi** | **status** | **tspec**}

Syntax Description

qos-map	Displays information about the QoS and 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 the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming failure.
rssi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays status of voice diagnostics for clients.
tspec	Displays voice diagnostics that are enabled for TSPEC clients.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Debug voice diagnostics must be enabled for voice diagnostics to work.

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Device# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```

show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command in privileged EXEC mode.

show wireless country {**channels**| **configured**| **supported [tx-power]**}

Syntax Description

channels	Displays the list of possible channels for each band, and the list of channels allowed in the configured countries.
configured	Display configured countries.
supported tx-power	Displays the list of allowed Tx powers in each supported country.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless country channels** command:

```
Device# show wireless country channels
  Configured Country.............................: US  - United States
      KEY: * = Channel is legal in this country and may be configured manually.
           A = Channel is the Auto-RF default in this country.
           . = Channel is not legal in this country.
           C = Channel has been configured for use by Auto-RF.
           x = Channel is available to be configured for use by Auto-RF.
         (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
```

```
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
    802.11bg     :
    Channels     :                   1 1 1 1 1
                 : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 (-A   ,-AB  )  US  :  A * * * * A * * * * A . . .
 Auto-RF         : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

```
(-E   ,-E   )  ES  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  FI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  FR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  GB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  GI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  GR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  HK  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-    )  HR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  HU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  ID  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-IE  )  IL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
(-A   ,-AN  )  IN  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  IQ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  IT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  J2  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPU ,-JPU )  J3  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU,-PQ  )  J4  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E   ,-    )  JO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-JPU ,-JPU )  JP  :  23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE ,-ACEK)  KE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-ACE ,-ACEK)  KR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KW  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  KZ  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LB  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  LK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  LV  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MC  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ME  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  MT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  MX  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-ACE ,-AEC )  MY  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  NO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-NA  )  NZ  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  OM  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AR  )  PA  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  PE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-ABN )  PH2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  PL  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PR  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  PT  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-A   )  PY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  QA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RO  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  RS  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AER ,-ER  )  RU  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-AE  ,-AE  )  SA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SE  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-SE  )  SG  :  20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E   ,-E   )  SI  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  SK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-ER  )  TH  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  TN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-EI  ,-E   )  TR  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-ANT )  TW  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-E   ,-E   )  UA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-A   ,-AB  )  US  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  US2 :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-A   )  UY  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-AR  )  VE  :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
```

```
(-E   ,-E   )  VN  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,-E   )  ZA  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
```

show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

show wireless detail

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

The following is sample output from the **show wireless detail** command:

```
Device# show wireless detail
User Timeout                : 300
RF network                  : default
Fast SSID                   : Disabled
```

show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

show wireless dtls connections

Syntax Description

This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless dtls connections** command:

```
Device# show wireless dtls connections
 AP Name         Local Port   Peer IP    Peer Port  Ciphersuite
----------------------------------------------------------------------
  AP-2       Capwap_Ctrl   10.0.0.16     52346      TLS_RSA_WITH_AES_128_CBC_SHA
  AP-3       Capwap_Ctrl   10.0.0.17     52347      TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless flow-control

To display the information about flow control on a particular channel, use the **show wireless flow-control** command in privileged EXEC mode.

show wireless flow-control *channel-id*

Syntax Description

channel-id	Identification number for a channel through which flow control is monitored.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show wireless flow-control** *channel-id* command:

```
Device# show wireless flow-control 3
Channel Name                          : CAPWAP
FC State                              : Disabled
```

```
Remote Server State                    : Enabled
Pass-thru Mode                         : Disabled
EnQ Disabled                           : Disabled
Queue Depth                            : 2048
Max Retries                            : 5
Min Retry Gap (mSec)                   : 3
```

show wireless flow-control statistics

To display the complete information about flow control on a particular channel, use the **show wireless flow-control statistics** command in privileged EXEC mode.

show wireless flow-control *channel-id* **statistics**

Syntax Description

channel-id	Identification number for a channel through which flow control is monitored.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show wireless flow-control** *channel-id* **statistics** command:

```
Device# show wireless flow-control 3 statistics
 Channel Name                                : CAPWAP
# of times channel went into FC              : 0
# of times channel came out of FC            : 0
Total msg count received by the FC Infra     : 1
Pass-thru msgs send count                    : 0
Pass-thru msgs fail count                    : 0
# of msgs successfully queued                : 0
# of msgs for which queuing failed           : 0
# of msgs sent thru after queuing            : 0
# of msgs sent w/o queuing                   : 1
# of msgs for which send failed              : 0
# of invalid EAGAINS received                : 0
Highest watermark reached                    : 0
# of times Q hit max capacity                : 0
Avg time channel stays in FC (mSec)          : 0
```

show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

show wireless load-balancing

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless load-balancing** command:

```
 > show wireless load-balancing
Aggressive Load Balancing.........................: per WLAN enabling
Aggressive Load Balancing Window (clients)................:: 5
Aggressive Load Balancing Denial Count....................:: 3

Statistics
Total Denied Count (clients)..............................:: 0
Total Denial Sent (messages)..............................:: 0
Exceeded Denial Max Limit Count (times)...................:: 0
None 5G Candidate Count (times)...........................:: 0
None 2.4G Candidate Count (times)........................:: 0
```

show wireless performance

To display aggressive load balancing configuration, use the **show wireless performance** command in privileged EXEC mode.

show wireless performance {**ap**| **client**} **summary**

Syntax Description

ap summary	Displays aggressive load balancing configuration of access points configured to the controller.
client summary	Displays aggressive load balancing configuration details of the clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless performance ap summary** command.

```
Device# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Device# show wireless performance client summary
Number of Clients:

MAC Address        AP Name           Status        WLAN/Guest-Lan Auth Protocol Port Wired
-------------------------------------------------------------------------------------------
```

show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

show wireless pmk-cache[**mac-address** *mac-addr*]

Syntax Description

mac-address *mac-addr*	(Optional) Information about a single entry in the PMK cache.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Device# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

To display the advanced probe request filtering configuration and the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show wireless probe** command in privileged EXEC mode.

show wireless probe

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless probe** command:

```
Device# show wireless probe
Probe request filtering                          : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval             : 500 msec
Aggregate probe request interval                 : 500 msec
```

show wireless sip preferred-call-no

To display SIP preferred call numbers, use the **show wireless sip preferred-call-no** command in privileged EXEC mode.

show wireless sip preferred-call-no

Syntax Description

This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless sip preferred-call-no** command:

```
Device# show wireless sip preferred-call-no
Index Preferred-Number
----------------------
1     1031
2     1032
4     1034
```

show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

show wireless summary

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

The following is sample output from the **show wireless summary** command:

```
Device# show wireless summary

Access Point Summary
```

```
               Total    Up    Down
-----------------------------------
802.11a/n          2     2       0
802.11b/g/n        2     2       0
All APs            2     2       0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

shutdown

To shut down VLAN switching, use the **shutdown** command in global configuration mode. To disable the configuration set, use the **no** form of this command.

shutdown [**vlan** *vlan-id*]

no shutdown

Syntax Description

vlan *vlan-id*	VLAN ID of VLAN to shutdown.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

This example shows how to shutdown a VLAN:

```
Device(config)# vlan open1
Device(config-wlan)# shutdown
```

This example shows that the access point is not shut down:

```
Device# configure terminal
Device(config)# ap name 3602a no shutdown
```

system env temperature threshold yellow

To configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold, use the **system env temperature threshold yellow** command in global configuration mode. To return to the default value, use the **no** form of this command.

system env temperature threshold yellow *value*

no system env temperature threshold yellow *value*

Syntax Description

value	Specifies the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25.

Command Default

These are the default values

Table 39: Default Values for the Temperature Thresholds

Device	Difference between Yellow and Red	Red[5]
Catalyst 3850	14°C	60°C

5 You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

Note The internal temperature sensor in the device measures the internal system temperature and might vary ±5 degrees C.

Example

This example sets 15 as the difference between the yellow and red thresholds:

```
Device(config)# system env temperature threshold yellow 15
Device(config)#
```

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Syntax Description

interface-id	The interface on which to run TDR.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

This example shows how to run TDR on an interface:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has an link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] **[detail]**

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination device.
source-mac-address	The MAC address of the source device in hexadecimal format.
destination-mac-address	The MAC address of the destination device in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devicees in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devicees:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devicees belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace aborted.
```

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} **[detail]**

Syntax Description

source-ip-address	The IP address of the source device as a 32-bit quantity in dotted-decimal format.
source-hostname	The IP hostname of the source device.

destination-ip-address	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
destination-hostname	The IP hostname of the destination device.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

trapflags

To enable sending rogue access point detection traps, use the **trapflags** command in privileged EXEC mode. To disable sending rogue access point detection traps, use the **no** form of this command.

trapflags rogueap

no trapflags rogueap

Syntax Description

rogueap	Enables sending rogue access point detection traps.

Command Default Enabled.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable the sending of rogue access point detection traps:

```
Device# configure terminal
Device(config)# no trapflags rogueap
Device(config)# end
```

trapflags client

To enable the sending of client-related DOT11 traps, use the **trapflags client** command in privileged EXEC mode. To disable the sending of client-related DOT11 traps, use the **no** form of this command.

trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

no trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

Syntax Description

dot11	Client-related DOT11 traps.
assocfail	Enables the sending of Dot11 association fail traps to clients.
associate	Enables the sending of Dot11 association traps to clients.
authfail	Enables the sending of Dot11 authentication fail traps to clients.
deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
disassociate	Enables the sending of Dot11 disassociation traps to clients.
excluded	Enables the sending of excluded trap to clients.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable the sending of Dot11 disassociation trap to clients:

```
Device# configure terminal
Device(config)# trapflags client dot11 disassociate
Device(config)# end
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appear sequentially.

Example

This example shows how to display the contents of a file:

```
Device: type flash:image_file_name
```

```
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset *variable...*

Syntax Description

variable	Use one of these keywords for *variable*: **MANUAL_BOOT—**Specifies whether the device automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.
	ENABLE_BREAK—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized.
	HELPER—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—Specifies the string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Example

This example shows how to display the boot loader version on a device:

```
Device: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.3, RELEASE SOFTWARE (P)
Compiled Sun Jun 16 18:31:15 PDT 2013 by rel
```

wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

wireless client {**association limit** *assoc-number* **interval** *interval*| **band-select** {**client-rssi** *rssi*| **cycle-count** *count*| **cycle-threshold** *threshold*| **expire dual-band** *timeout*| **expire suppression** *timeout*}| **max-user-login** *max-user-login*| **timers auth-timeout** *seconds*| **user-timeout** *user-timeout*}

Syntax Description

association limit *assoc-number* **interval** *interval*	Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.
band-select	Configures band select options for the client.
client-rssi *rssi*	Sets the client received signal strength indicator (RSSI) threshold for band select. Minimum dBm of a client RSSI to respond to probe between -90 and -20.
cycle-count *count*	Sets the band select probe cycle count. You can configure the cycle count from one through 10.
cycle-threshold *threshold*	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from one through 1000 milliseconds.
expire dual-band *timeout*	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 through 300 seconds, and the default value is 60 seconds.
expire suppression *timeout*	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 through 200 seconds, and the default timeout value is 20 seconds.

max-user-login *max-user-login*	Configures the maximum number of login sessions for a user.
timers auth-timeout *seconds*	Configures client timers.
user-timeout *user-timeout*	Configures the idle client timeout.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to set the proble cycle count for band select to 8:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 8
Device(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Device# configure terminal
Device(config)# wireless client band-select cycle-threshold 700
Device(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(config)# end
```

wireless client mac-address deauthenticate

To disconnect a wireless client, use the **wireless client mac-address deauthenticate** command in global configuration mode.

wirelessclientmac-address *mac-addr***deauthenticate**

Syntax Description

mac-address *mac-addr*	Wireless client MAC address.

Command Default No default behavior or values.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disconnect a wireless client:

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Device(config)# end
```

wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

wireless client mac-address *mac-addr* **ccx** {**clear-reports**| **clear-results**| **default-gw-ping**| **dhcp-test**| **dns-ping**| **dns-resolve hostname** *host-name*| **get-client-capability**| **get-manufacturer-info**| **get-operating-parameters**| **get-profiles**| **log-request** {**roam**| **rsna**| **syslog**}| **send-message** *message-id*| **stats-request** *measurement-duration* {**dot11**| **security**}| **test-abort**| **test-association** *ssid bssid dot11 channel*| **test-dot1x** [*profile-id*] *bssid dot11 channel*| **test-profile** {**any**| *profile-id*}}

Syntax Description

mac-addr	MAC address of the client.
ccx	Cisco client extension (CCX).
clear-reports	Clears the client reporting information.
clear-results	Clears the test results on the controller.
default-gw-ping	Sends a request to the client to perform the default gateway ping test.
dhcp-test	Sends a request to the client to perform the DHCP test.
dns-ping	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
dns-resolve hostname *host-name*	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.

get-client-capability	Sends a request to the client to send its capability information.
get-manufacturer-info	Sends a request to the client to send the manufacturer's information.
get-operating-parameters	Sends a request to the client to send its current operating parameters.
get-profiles	Sends a request to the client to send its profiles.
log-request	Configures a CCX log request for a specified client device.
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.

send-message *message-id*

Sends a message to the client.

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.

	• 31—The WLAN security method is not correct. • 32—The WLAN encryption method is not correct. • 33—The WLAN authentication method is not correct.
stats-request *measurement-duration*	Senda a request for statistics.
dot11	Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
test-abort	Sends a request to the client to abort the current test.
test-association *ssid bssid dot11 channel*	Sends a request to the client to perform the association test.
test-dot1x	Sends a request to the client to perform the 802.1x test.
profile-id	(Optional) Test profile name.
bssid	Basic SSID.
dot11	Specifies the 802.11a, 802.11b, or 802.11g network.
channel	Channel number.
test-profile	Sends a request to the client to perform the profile redirect test.
any	Sends a request to the client to perform the profile redirect test.
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

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **default-gw-ping** test does not require the client to use the diagnostic channel.

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(config)# end
```

wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

wireless load-balancing {**denial** *denial-count*| **window** *client-count*}

Syntax Description

denial *denial-count*	Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
window *client-count*	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

Command Default

Disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

This example shows how to configure association denials during load balancing:

```
Device# configure terminal
Device(config)# wireless load-balancing denial 5
Device(config)# end
```

wireless sip preferred-call-no

To add a new preferred call or configure voice prioritization, use the **wireless sip preferred-call-no** command in global configuration mode. To remove a preferred call, use the **no** form of this command.

wireless sip preferred-call-no *callIndex call-no*

no wireless sip preferred-call-no *callIndex*

Syntax Description

callIndex	Call index with valid values between 1 and 6.
call-no	Preferred call number that can contain up to 27 characters.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Before you configure voice prioritization, you must complete the following prerequisites:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

This example shows how to add a new preferred call or configure voice prioritization:

```
Device# configure terminal
Device(config)# wireless sip preferred-call-no 2 0123456789
Device(config)# end
```

CHAPTER 16

Tracing Commands

- Information About Tracing, page 911
- set platform software trace, page 913
- show platform software trace filter-binary, page 917
- show platform software trace message, page 918
- show platform software trace level, page 921
- request platform software trace archive, page 924
- request platform software trace rotate all, page 925
- request platform software trace filter-binary, page 925

Information About Tracing

Tracing Overview

The tracing functionality logs internal events. Trace files are automatically created and saved to the tracelogs subdirectory under crashinfo.

The contents of trace files are useful for the following purposes:

- Troubleshooting—If a switch has an issue, the trace file output may provide information that can be used for locating and solving the issue.
- Debugging—The trace file outputs helps users get a more detailed view of system actions and operations.

To view the most recent trace information for a specific module, use the **show platform software trace message** command.

To modify the trace level to increase or decrease the amount of trace message output, you can set a new trace level using the **set platform software trace** command. Trace levels can be set for each process using the **all-modules** keyword in the **set platform software trace** command, or per module within a process.

Location of Tracelogs

Each process uses btrace infrastructure to log its trace messages. When a process is active, the corresponding in-memory tracelog is found in the directory `/tmp/<FRU>/trace/`, where <FRU> refers to the location where the process is running (rp, fp, or cc).

When a tracelog file has reached the maximum file size limit allowed for the process, or if the process ends, it gets rotated into the following directory:

- /crashinfo/tracelogs, if the crashinfo: partition is available on the switch
- /harddisk/tracelogs, if the crashinfo: partition is not available on the switch

The tracelog files are compressed before being stored in the directory.

Tracelog Naming Convention

All the tracelogs that are created using btrace have the following naming convention:

`<process_name>_<FRU><SLOT>-<BAY>.<pid>_<counter>.<creation_timestamp>.bin`

Here, counter is a free-running 64-bit counter that gets incremented for each new file created for the process. For example, wcm_R0-0.1362_0.20151006171744.bin. When compressed, the files will have the gz extension appended to their names

Tracelog size limits and rotation policy

The maximum size limit for a tracelog file is 1MB for each process, and the maximum number of tracelog files that are maintained for a process is 25.

Rotation and Throttling Policy

Initially, all the tracelog files are moved from the initial `/tmp/<FRU>/trace` directory to the `/tmp/<FRU>/trace/stage` staging directory. The `btrace_rotate` script then moves these tracelogs from the staging directory to the `/crashinfo/tracelogs` directory. When the number of files stored in the `/crashinfo/tracelogs` directory per process reaches the maximum limit, the oldest files for the process are deleted, while the newer files are maintained. This is repeated at every 60 minutes under worst-case situations.

There are two other sets of files that are purged from the `/crashinfo/tracelogs` directory:

- Files that do not have the standard naming convention (other than a few exceptions such as `fed_python.log`)
- Files older than two weeks

The throttling policy has been introduced so that a process with errors does not affect the functioning of the switch. Whenever a process starts logging at a very high rate, for example, if there are more than 16 files in a 4-second interval for the process in the staging directory, the process is throttled. The files do not rotate for the process from `/tmp/<FRU>/trace` into `/tmp/<FRU>/trace/stage`, however the files are deleted when they reach the maximum size. Throttling is re-enabled, when the count goes below 8.

Tracing Levels

Tracing levels determine how much information should be stored about a module in the trace buffer or file.

The following table shows all of the tracing levels that are available, and provides descriptions of the message that are displayed with each tracing level.

Table 40: Tracing Levels and Descriptions

Tracing Level	Description
Emergency	The message is regarding an issue that makes the system unusable.
Error	The message is regarding a system error.
Warning	The message is regarding a system warning.
Notice	The message is regarding a significant issue, but the switch is still working normally.
Informational	The message is useful for informational purposes only.
Debug	The message provides debug-level output.
Verbose	All possible trace messages are sent.
Noise	All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

set platform software trace

To set the trace level for a specific module within a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

set platform software trace *process slot module trace-level*

Syntax Description

process	Process whose tracing level is being set. Options include: • **chassis-manager—**The Chassis Manager process. • **cli-agent—**The CLI Agent process. • **dbm—**The Database Manager process. • **emd—**The Environmental Monitoring process. • **fed—**The Forwarding Engine Driver process. • **forwarding-manager—**The Forwarding Manager process. • **host-manager—**The Host Manager process. • **iomd—**The Input/Output Module daemon (IOMd) process. • **ios—**The IOS process. • **license-manager—**The License Manager process. • **logger—**The Logging Manager process. • **platform-mgr—**The Platform Manager process. • **pluggable-services—**The Pluggable Services process. • **replication-mgr—**The Replication Manager process. • **shell-manager—**The Shell Manager process. • **smd—**The Session Manager process. • **table-manager—**The Table Manager Server. • **wireless—**The wireless controller module process. • **wireshark—**The Embedded Packet Capture (EPC) Wireshark process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include: • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • **F0**—The Embedded-Service-Processor in slot 0. • **FP active**—The active Embedded-Service-Processor. • **R0**—The route processor in slot 0. • **RP active**—The active route processor. • **switch** <*number*> —The switch with its number specified. • **switch active**—The active switch. • **switch standby**—The standby switch.
module	Module within the process for which the tracing level is set.

trace-level	Trace level. Options include: • **debug—**Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module. • **emergency—**Emergency level tracing. An emergency-level trace message is a message indicating that the system is unusable. • **error—**Error level tracing. An error-level tracing message is a message indicating a system error. • **info—**Information level tracing. An information-level tracing message is a non-urgent message providing information about the system. • **noise—**Noise level tracing. The noise level is always equal to the highest tracing level possible and always generates every possible tracing message. The noise level is always equal to the highest-level tracing message possible for a module, even if future enhancements to this command introduce options that allow users to set higher tracing levels. • **notice—**The message is regarding a significant issue, but the switch is still working normally. • **verbose—**Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose. • **warning—**Warning messages.

Command Default

The default tracing level for all modules is **notice**.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The *module* options vary by process and by *hardware-module*. Use the ? option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the tracelogs directory in the harddisk: file system. These files can be deleted without doing any harm to your switch operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information should be stored in trace files about a module.

Example

This example shows how to set the trace level for all the modules in dbm process:

```
Device# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

show platform software trace filter-binary*modules* [**context** *mac-address*]

Syntax Description

context*mac-address*	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command collates and sorts all the logs present in the `/tmp/.../` across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.

Example

This example shows how to display the trace information for a wireless module:

```
Device# show platform software trace filter-binary wireless
```

show platform software trace message

To display the trace messages for a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

show platform software trace message *process slot*

Syntax Description

process	Tracing level that is being set. Options include: • **chassis-manager—**The Chassis Manager process. • **cli-agent—**The CLI Agent process. • **cmm—**The CMM process. • **dbm—**The Database Manager process. • **emd—**The Environmental Monitoring process. • **fed—**The Forwarding Engine Driver process. • **forwarding-manager—**The Forwarding Manager process. • **geo—**The Geo Manager process. • **host-manager—**The Host Manager process. • **interface-manager—**The Interface Manager process. • **iomd—**The Input/Output Module daemon (IOMd) process. • **ios—**The IOS process. • **license-manager—**The License Manager process. • **logger—**The Logging Manager process. • **platform-mgr—**The Platform Manager process. • **pluggable-services—**The Pluggable Services process. • **replication-mgr—**The Replication Manager process. • **shell-manager—**The Shell Manager process. • **sif—**The Stack Interface (SIF) Manager process. • **smd—**The Session Manager process. • **stack-mgr—**The Stack Manager process. • **table-manager—**The Table Manager Server. • **thread-test—**The Multithread Manager process. • **virt-manager—**The Virtualization Manager process. • **wireless—**The wireless controller module process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include: • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • **F0**—The Embedded Service Processor slot 0. • **FP active**—The active Embedded Service Processor. • **R0**—The route processor in slot 0. • **RP active**—The active route processor. • **switch** <*number*> —The switch, with its number specified. • **switch active**—The active switch. • **switch standby**—The standby switch. ◦ *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. ◦ *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. ◦ **F0**—The Embedded Service Processor in slot 0. ◦ **FP active**—The active Embedded Service Processor. ◦ **R0**—The route processor in slot 0. ◦ **RP active**—The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Single message size is greater
 than 1024
11/02 10:55:01.822 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]:  UUID: 0, ra: 0 (note): Successfully registered module
 [89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]:  UUID: 0, ra: 0 (note): Successfully registered module
 [90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]:  UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]:  UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
 result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
 failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]:  UUID: 0, ra: 0 (ERR):
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

show platform software trace level *process slot*

Syntax Description

process	Process whose tracing level is being set. Options include: • **chassis-manager—**The Chassis Manager process. • **cli-agent—**The CLI Agent process. • **cmm—**The CMM process. • **dbm—**The Database Manager process. • **emd—**The Environmental Monitoring process. • **fed—**The Forwarding Engine Driver process. • **forwarding-manager—**The Forwarding Manager process. • **geo—**The Geo Manager process. • **host-manager—**The Host Manager process. • **interface-manager—**The Interface Manager process. • **iomd—**The Input/Output Module daemon (IOMd) process. • **ios—**The IOS process. • **license-manager—**The License Manager process. • **logger—**The Logging Manager process. • **platform-mgr—**The Platform Manager process. • **pluggable-services—**The Pluggable Services process. • **replication-mgr—**The Replication Manager process. • **shell-manager—**The Shell Manager process. • **sif—**The Stack Interface (SIF) Manager process. • **smd—**The Session Manager process. • **stack-mgr—**The Stack Manager process. • **table-manager—**The Table Manager Server. • **thread-test—**The Multithread Manager process. • **virt-manager—**The Virtualization Manager process. • **wireless—**The wireless controller module process.

slot	Hardware slot where the process for which the trace level is set, is running. Options include: • *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • **F0—**The Embedded Service Processor in slot 0. • **F1—**The Embedded Service Processor in slot 1. • **FP active—**The active Embedded Service Processor. • **R0—**The route processor in slot 0. • **RP active—**The active route processor. • **switch** <*number*> **—**The switch, with its number specified. • **switch active—**The active switch. • **switch standby—**The standby switch. ◦ *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. ◦ *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. ◦ **F0—**The Embedded Service Processor in slot 0. ◦ **FP active—**The active Embedded Service Processor. ◦ **R0—**The route processor in slot 0. ◦ **RP active—**The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
Module Name                      Trace Level
----------------------------------------------
binos                            Notice
binos/brand                      Notice
bipc                             Notice
btrace                           Notice
bump_ptr_alloc                   Notice
cdllib                           Notice
chasfs                           Notice
dbal                             Informational
dbm                              Debug
evlib                            Notice
evutil                           Notice
file_alloc                       Notice
green-be                         Notice
ios-avl                          Notice
klib                             Debug
services                         Notice
sw_wdog                          Notice
syshw                            Notice
tdl_cdlcore_message              Notice
tdl_dbal_root_message            Notice
tdl_dbal_root_type               Notice
```

request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the switches and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

request platform software trace archive [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

Syntax Description

last *number-of-days*	Specifies the number of days for which the trace files have to be archived.
target *location*	Specifies the location and name of the archive file.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This archive file can be copied from the system, using the tftp or scp commands.

Example

This example shows how to archive all the trace logs of the processes running on the switch since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

To rotate all the current in-memory trace logs into the crashinfo partition and start a new in-memory trace log for each process, use the **request platform software trace rotate all** command in privileged EXEC or user EXEC mode.

request platform software trace rotate all

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The trace log files are for read-only purpose. Do not edit the contents of the file. If there is a requirement to delete the contents of the file to view certain set of logs, use this command to start a new trace log file.

Example

This example shows how to rotate all the in-memory trace logs of the processes running on the switch since the last one day:

```
Device# request platform software trace slot switch active R0 archive last 1 days target
flash:test
```

request platform software trace filter-binary

To collate and sort all the archived logs present in the tracelogs subdirectory, use the **request platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

request platform software trace filter-binary *modules* [**context** *mac-address*]

Syntax Description

context *mac-address*	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command collates and sorts all the archived logs present in the tracelogs subdirectory, across all the processes relevant to the module. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.

Example

This example shows how to display the trace information for a wireless module:

```
Device# request platform software trace filter-binary wireless
```

PART XV

VideoStream

- VideoStream Commands, page 929

CHAPTER 17

VideoStream Commands

- ap dot11 media-stream multicast-direct, page 929
- show ap dot11, page 930
- show wireless media-stream group, page 931
- wireless media-stream multicast-direct, page 932
- wireless media-stream, page 933

ap dot11 media-stream multicast-direct

To configure multicast-direct for 2.4-GHz/5-GHz band, use the **ap dot11 media-stream multicast-direct** command.

ap dot11 {**24ghz**| **5ghz**} **media-stream** {**multicast-direct** {**admission-besteffort**| **client-maximum** *value*| **radio-maximum** *value*}| **video-redirect**}

Syntax Description

multicast-direct	Configure multicast-direct for 802.11 band
admission-besteffort	Admits media stream to best-effort queue.
client-maximum *value*	Specifies the maximum number of streams allowed on a client.
radio-maximum *value*	Specifies the maximum number of streams allowed on a 2.4-GHz or a 5-GHz band.
video-redirect	Redirect non Multicast-direct video to BestEffort queue over the air.

Command Default

None

Command Modes config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

Examples

The following example shows how to configure multicast-direct for the 2.4-GHz band.

```
(Cisco Controller) >Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#ap dot11 24ghz media-stream multicast-direct
```

show ap dot11

To display 802.11 band parameters, use the **show ap dot11** command.

show ap dot11 {**24ghz**| **5ghz**} {**media-stream rrc**| **network**| **profile**| **summary**}

Syntax Description

media-stream rrc	Displays Media Stream configurations.
network	Shows network configuration.
profile	Shows profiling information for all Cisco APs.
summary	Shows configuration and statistics of 802.11b and 802.11a Cisco APs.

Command Default None

Command Modes User EXEC command mode or Privileged EXEC command mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Command History

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

Usage Guidelines

None.
The following is a sample output of the **show ap dot11 24ghz media-stream rrc** command.

```
Device#show ap dot11 24ghz media-stream rrc

Multicast-direct                 : Disabled
Best Effort                      : Disabled
Video Re-Direct                  : Disabled
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 (Kbps)               : 6000
Max Retry Percentage              : 80
```

show wireless media-stream group

To display the wireless media-stream group information, use the **show wireless media-stream group** command.

show wireless media-stream group {**detail** *groupName*| **summary**}

Syntax Description

detail *groupName*	Display media-stream group configuration details of the group mentioned in the command.
summary	Display media-stream group configuration summary

Command Default

None

Command Modes

User EXEC mode or Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Command History

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

Usage Guidelines

None.

The following is a sample output of the **show wireless media-stream group detail GRP1** command.

```
Device#show wireless media-stream group detail GRP1
```

wireless media-stream multicast-direct

To configure multicast-direct status, use the **media-stream multicast-direct** command. To remove the multicast-direct status, use the no form of the command.

no wireless media-stream multicast-direct

Command Default

None

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

Examples

The following example shows how to configure multicast-direct for a wireless LAN media stream.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless media-stream multicast-direct
```

wireless media-stream

To configure various parameters, use the **wireless media-stream** command.

wireless media-stream group *groupName* [*startipAddr endipAddr*]

wireless media-stream group{ avg-packet-size default exit max-bandwidth no policy qos}

wireless media-stream {**multicast-direct**| **message** [**phone** *phone*| **URL** *URL*| **Notes** *Notes*| **Email** *Email*]}

Syntax Description

group *groupName*	Configure multicast-direct status for a group.
startipAddr	Specifies the start IP Address for the group.
endipAddr	Specifies the End IP Address for the group.
group *avg-packet-size*	Configure average packet size.
group *default*	Set a command to its defaults.
group *exit*	Exit sub-mode.
group *max-bandwidth*	Configure maximum expected stream bandwidth in Kbps.
group *no*	Negate a command or set its defaults.
group *policy*	Configure media stream admission policy.
group *qos*	Configure over the air QoS class, <'video'> ONLY.
multicast-direct	Configure multicast-direct status.
message	Configure Session Announcement Message.
phone *phone*	Configure Session Announcement Phone number.
URL *URL*	Configure Session Announcement URL.
Notes *Notes*	Configure Session Announcement notes.
Email *Email*	Configure Session Announcement Email.

Command Default

Disabled

Command Modes

config

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

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.

Examples

The following example shows how to configure each media stream and its parameters like expected multicast destination addresses, stream bandwidth consumption and stream priority parameters.

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```

PART XVI

VLAN

- VLAN Commands, page 937

CHAPTER 18

VLAN Commands

- client vlan, page 938
- clear vtp counters, page 939
- debug platform vlan, page 939
- debug sw-vlan, page 940
- debug sw-vlan ifs, page 941
- debug sw-vlan notification, page 942
- debug sw-vlan vtp, page 943
- interface vlan, page 945
- show platform vlan, page 946
- show vlan, page 946
- show vtp, page 949
- show wireless vlan group, page 955
- switchport priority extend, page 956
- switchport trunk, page 957
- vlan, page 959
- vlan dot1q tag native, page 965
- vtp (global configuration), page 965
- vtp (interface configuration), page 970
- vtp primary, page 971
- wireless broadcast vlan, page 972

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*

no client vlan

Syntax Description

interface-id-name-or-group-name	Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default

The default interface is configured.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to clear the VTP counters:

```
Device# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

debug platform vlan

To enable debugging of the VLAN manager software, use the **debug platform vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug platform vlan [**error**| **event**] [**switch** *switch-number*]

no debug platform vlan [**error**| **event**] [**switch** *switch-number*]

Syntax Description

error	(Optional) Displays VLAN error debug messages.
event	(Optional) Displays VLAN platform event debug messages.
switch *switch-number*	(Optional) Specifies the stack member number on which to enable debugging of the VLAN manager software. This keyword is supported only on stacking-capable switches.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

This example shows how to display VLAN error debug messages:

```
Device# debug platform vlan error
```

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **management**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

no debug sw-vlan {**badpmcookies**| **cfg-vlan** {**bootup**| **cli**}| **events**| **ifs**| **management**| **mapping**| **notification**| **packets**| **redundancy**| **registries**| **vtp**}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 941 for more information.
management	Displays debug messages for VLAN manager management of internal VLANs.
mapping	Displays debug messages for VLAN mapping.
notification	Displays debug messages for VLAN manager notifications. See debug sw-vlan notification, on page 942 for more information.

packets	Displays debug messages for packet handling and encapsulation processes.
redundancy	Displays debug messages for VTP VLAN redundancy.
registries	Displays debug messages for VLAN manager registries.
vtp	Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 943 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

This example shows how to display debug messages for VLAN manager events:

```
Device# debug sw-vlan events
```

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

no debug sw-vlan ifs {**open** {**read**| **write**}| **read** {**1**| **2**| **3**| **4**}| **write**}

Syntax Description

open read	Displays VLAN manager IFS file-read operation debug messages.
open write	Displays VLAN manager IFS file-write operation debug messages.
read	Displays file-read operation debug messages for the specified error test (**1**, **2**, **3**, or **4**).

write	Displays file-write operation debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

This example shows how to display file-write operation debug messages:

```
Device# debug sw-vlan ifs write
```

debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {**accfwdchange**| **allowedvlancfgchange**| **fwdchange**| **linkchange**| **modechange**| **pruningcfgchange**| **statechange**}

no debug sw-vlan notification {**accfwdchange**| **allowedvlancfgchange**| **fwdchange**| **linkchange**| **modechange**| **pruningcfgchange**| **statechange**}

Syntax Description

accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.
allowedvlancfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.

linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.
modechange	Displays debug messages for VLAN manager notification of interface mode changes.
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.
statechange	Displays debug messages for VLAN manager notification of interface state changes.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Device# debug sw-vlan notification
```

debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan vtp {**events**| **packets**| **pruning** [**packets**| **xmit**]| **redundancy**| **xmit**}

no debug sw-vlan vtp {**events**| **packets**| **pruning**| **redundancy**| **xmit**}

Syntax Description

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.

packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
redundancy	Displays debug messages for VTP redundancy.
xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no additional parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch** *stack-member-number* privileged EXEC command.

This example shows how to display debug messages for VTP redundancy:

```
Device# debug sw-vlan vtp redundancy
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*

no interface vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

Note When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.

Note You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

show platform vlan

To display platform-dependent VLAN information, use the **show platform vlan** privileged EXEC command.

show platform vlan [*vlan-id*] [**switch** *switch-number*]

Syntax Description

vlan-id	(Optional) ID of the VLAN. The range is 1 to 4094.
switch *switch-number*	(Optional) Limits the display to VLANs on the specified stack member.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

This example shows how to display platform-dependent VLAN information:

```
Device# show platform vlan
```

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

show vlan [**brief**| **dot1q tag native**| **group**| **id** *vlan-id*| **mtu**| **name** *vlan-name*| **remote-span**| **summary**]

Syntax Description

brief	(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.

dot1q tag native	(Optional) Displays the IEEE 802.1Q native VLAN tagging status.
group	(Optional) Displays information about VLAN groups.
id *vlan-id*	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For *vlan-id*, the range is 1 to 4094.
mtu	(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.
name *vlan-name*	(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.
remote-span	(Optional) Displays information about Remote SPAN (RSPAN) VLANs.
summary	(Optional) Displays VLAN summary information.

Note The **ifindex** keyword is not supported, even though it is visible in the command-line help string.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When yes appears in the column, it means that the VLAN has ports with different MTUs, and packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have an SVI, the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays yes, the names of the ports with the MinMTU and the MaxMTU appear.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Device> show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
```

```
                                                    Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                    Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                    Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                    Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                    Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                    Gi1/0/23, Gi1/0/24, Gi1/0/25
                                                    Gi1/0/26, Gi1/0/27, Gi1/0/28
                                                    Gi1/0/29, Gi1/0/30, Gi1/0/31
                                                    Gi1/0/32, Gi1/0/33, Gi1/0/34
                                                    Gi1/0/35, Gi1/0/36, Gi1/0/37
                                                    Gi1/0/38, Gi1/0/39, Gi1/0/40
                                                    Gi1/0/41, Gi1/0/42, Gi1/0/43
                                                    Gi1/0/44, Gi1/0/45, Gi1/0/46
                                                    Gi1/0/47, Gi1/0/48
2    VLAN0002                          active
40   vlan-40                           active
300  VLAN0300                          active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
2    enet  100002     1500  -      -      -        -    -        0      0
40   enet  100040     1500  -      -      -        -    -        0      0
300  enet  100300     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0
2000 enet  102000     1500  -      -      -        -    -        0      0
3000 enet  103000     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
------------------------------------------------------------------------------
2000,3000

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Table 41: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.

Field	Description
BrdgNo	Bridge number for the VLAN, if applicable.
Stp	Spanning Tree Protocol type used on the VLAN.
BrdgMode	Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.
Trans1	Translation bridge 1.
Trans2	Translation bridge 2.
Remote SPAN VLANs	Identifies any RSPAN VLANs that have been configured.

This is an example of output from the **show vlan dot1q tag native** command:

```
Device> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan summary** command:

```
Device> show vlan summary
Number of existing VLANs               : 45
 Number of existing VTP VLANs          : 45
 Number of existing extended VLANS     : 0
```

This is an example of output from the **show vlan id** command:

```
Device# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    VLAN0200                         active    Gi1/0/7, Gi1/0/8
2    VLAN0200                         active    Gi2/0/1, Gi2/0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLANs
-------------------------------------------------------------------------------
Disabled
```

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

show vtp {**counters**| **devices** [**conflicts**]| **interface** [*interface-id*]| **password**| **status**}

Syntax Description

counters	Displays the VTP statistics for the device.
devices	Displays information about all VTP version 3 devices in the domain. This keyword applies only if the device is not running VTP version 3.

conflicts	(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the device is in VTP transparent or VTP off mode.
interface	Displays VTP status and configuration for all interfaces or the specified interface.
interface-id	(Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
password	Displays the configured VTP password (available in privileged EXEC mode only).
status	Displays general information about the VTP management domain status.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enter the **show vtp password** command when the device is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the device, the password appears in clear text.
- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the device, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

This is an example of output from the **show vtp devices** command. A Yes in the Conflict column indicates that the responding server is in conflict with the local server for the feature; that is, when two devices in the same domain do not have the same primary server for a database.

```
Device# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf device ID      Primary Server Revision   System Name
             lict
------------ ---- -------------- -------------- ---------- ----------------------
VLAN         Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST          No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
```

```
VLAN         Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Device> show vtp counters
VTP statistics:
Summary advertisements received    : 0
Subset advertisements received     : 0
Request advertisements received    : 0
Summary advertisements transmitted : 0
Subset advertisements transmitted  : 0
Request advertisements transmitted : 0
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received    Summary advts received from
                                                   non-pruning-capable device
---------------- ---------------- ---------------- ---------------------------
Gi1/0/47              0                0                0
Gi1/0/48              0                0                0
Gi2/0/1               0                0                0
Gi3/0/2               0                0                0
```

Table 42: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Summary advertisements transmitted	Number of summary advertisements sent by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.

Field	Description
Request advertisements transmitted	Number of advertisement requests sent by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the device increments. Revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of configuration digest errors	Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a device in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring device is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the devices in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.

Field	Description
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

```
Device> show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                                    0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 43: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the device.
VTP Version running	Displays the VTP version operating on the device. By default, the device implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the device.
VTP Pruning Mode	Displays whether pruning is enabled or disabled. Enabling pruning on a VTP server enables pruning for the entire management domain. Pruning restricts flooded traffic to those trunk links that the traffic must use to access the appropriate network devices.
VTP Traps Generation	Displays whether VTP traps are sent to a network management station.
Device ID	Displays the MAC address of the local device.

Field	Description
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the device that caused the configuration change to the database.
VTP Operating Mode	Displays the VTP operating mode, which can be server, client, or transparent. **Server—**A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The device guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every device is a VTP server. **Note** The device automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning. **Client—**A device in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database. **Transparent—**A device in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.
Configuration Revision	Current configuration revision number on this device.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a device running VTP version 3:

```
Device> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700
```

```
Feature VLAN:
--------------
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature MST:
--------------
VTP Operating Mode : Client
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00

Feature UNKNOWN:
----------------
```

show wireless vlan group

To display the detailed list of VLANs in a VLAN group and the status of the DHCP failed vlans, use the **show wireless vlan group** command in privileged EXEC mode.

show wireless vlan group *group-name*

Syntax Description

group-name	Name of the wireless VLAN group.

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enter this command in the global configuration mode only.

This example shows how to display the summary of a VLAN group:

```
Device# show wireless vlan group grp1

Member Vlans Configured
------------------------------------------------------------
VLAN        VLAN Name                          DHCP Failed
100         VLAN0100                           No
```

```
101         VLAN0101                         Yes
102         VLAN0102                         No
103         VLAN0103                         No
104         VLAN0104                         Yes
105         VLAN0105                         No
```

switchport priority extend

To set a port priority for the incoming untagged frames or the priority of frames received by the IP phone connected to the specified port, use the **switchport priority extend** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport priority extend {**cos** *value*| **trust**}

no switchport priority extend

Syntax Description

cos *value*	Sets the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.
trust	Sets the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.

Command Default

The default port priority is set to a CoS value of 0 for untagged frames received on the port.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When voice VLAN is enabled, you can configure the device to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the device port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all device interfaces.)

You should configure voice VLAN on device access ports. You can configure a voice VLAN only on Layer 2 ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the interface by entering the **trust device cisco-phone** interface configuration command. If you use the auto QoS feature, these settings are automatically configured.

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport priority extend trust
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

switchport trunk {**allowed vlan** *vlan-list*| **native vlan** *vlan-id*| **pruning vlan** *vlan-list*}

no switchport trunk {**allowed vlan**| **native vlan**| **pruning vlan**}

Syntax Description

allowed vlan *vlan-list*	Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.
native vlan *vlan-id*	Sets the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
pruning vlan *vlan-list*	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the *vlan-list* choices.

Command Default

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The *vlan-list* format is **all | none | [add | remove | except]** *vlan-atom* [,*vlan-atom*...]:

- **all** specifies all VLANs from 1 to 4094. This is the default. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.

- **none** specifies an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLANs (VLAN IDs greater than 1005) are valid in some cases.

  Note You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 1005; extended-range VLAN IDs are valid in some cases.

  Note You can remove extended-range VLANs from the allowed VLAN list, but you cannot remove them from the pruning-eligible list.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

Trunk pruning:

- The pruning-eligible list applies only to trunk ports.
- Each trunk port has its own eligibility list.
- If you do not want a VLAN to be pruned, remove it from the pruning-eligible list. VLANs that are pruning-ineligible receive flooded traffic.

- VLAN 1, VLANs 1002 to 1005, and extended-range VLANs (VLANs 1006 to 4094) cannot be pruned.

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*

no vlan *vlan-id*

Syntax Description

vlan-id	ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.
group **word vlan-list**	Enables creation of the VLAN group. The VLAN group name may contain up to 32 characters and must commence with a letter.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You can use the **vlan** *vlan-id* global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range

VLANs is always saved in the VLAN database, and you can display this information by entering the **show vlan** privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the device running configuration file. VLAN IDs in the extended range are not saved in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file.

VTP version 3 supports propagation of extended-range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

Note Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is **remote-span**. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state:

- **are** *are-number*—Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.
- **backupcrf**—Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable**—Backup CRF mode for this VLAN.
  - **disable**—Backup CRF mode for this VLAN (the default).
- **bridge** {*bridge-number* | **type**}—Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The **type** keyword applies only to TrCRF VLANs and is one of these:
  - **srb**—Ssource-route bridging
  - **srt**—Source-route transparent) bridging VLAN

- **exit—**Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media—**Defines the VLAN media type and is one of these:

  Note The device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.

  - **ethernet—**Ethernet media type (the default).
  - **fd-net—**FDDI network entity title (NET) media type.
  - **fddi—**FDDI media type.
  - **tokenring—**Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
  - **tr-net—**Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

  See the table that follows for valid commands and syntax for different media types.
- **name** *vlan-name***—**Names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is VLANxxxx where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no—**Negates a command or returns it to the default setting.
- **parent** *parent-vlan-id***—**Specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.
- **remote-span—**Configures the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN IDs that are lower than 1024. Learning is disabled on the VLAN.

  Note The RSPAN feature is supported only on switches running the LAN Base image.
- **ring** *ring-number***—**Defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095. The default for Token Ring VLANs is 0. For FDDI VLANs, there is no default.
- **said** *said-value***—**Specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown—**Shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.
- **state—**Specifies the VLAN state:

- **active** means the VLAN is operational (the default).
- **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.

- **ste** *ste-number*—Defines the maximum number of spanning-tree explorer (STE) hops. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**—Defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs. For FDDI-NET VLANs, the default STP type is ieee. For Token Ring-NET VLANs, the default STP type is ibm. For FDDI and Token Ring VLANs, the default is no type specified.
  - **ieee**—IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm**—IBM STP running source-route bridging (SRB).
  - **auto**—STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*—Specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.

Table 44: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	**name** *vlan-name*, **media ethernet**, **state** {**suspend** | **active**}, **said** *said-value*, **remote-span**, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI	**name** *vlan-name*, **media fddi**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
FDDI-NET	**name** *vlan-name*, **media fd-net** , **state** {**suspend** | **active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee** | **ibm** | **auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id* If VTP v2 mode is disabled, do not set the **stp type** to **auto.**
Token Ring	VTP v1 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend** | **active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

Media Type	Valid Syntax
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tokenring**, **state** {**suspend | active**}, **said** *said-value*, **ring** *ring-number*, **parent** *parent-vlan-id*, **bridge type** {**srb | srt**}, **are** *are-number*, **ste** *ste-number*, **backupcrf** {**enable | disable**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring-NET	VTP v1 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee | ibm**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. **name** *vlan-name*, **media tr-net**, **state** {**suspend | active**}, **said** *said-value*, **bridge** *bridge-number*, **stp type** {**ieee | ibm | auto**}, **tb-vlan1** *tb-vlan1-id*, **tb-vlan2** *tb-vlan2-id*

The following table describes the rules for configuring VLANs:

Table 45: VLAN Configuration Rules

Configuration	Rule
VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.	Specify a parent VLAN ID of a TrBRF that already exists in the database. Specify a ring number. Do not leave this field blank. Specify unique ring numbers when TrCRF VLANs have the same parent VLAN ID. Only one backup concentrator relay function (CRF) can be enabled.
VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.	Do not specify a backup CRF.
VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.	Specify a bridge number. Do not leave this field blank.
VTP v1 mode is enabled.	No VLAN can have an STP type set to auto. This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.

Configuration	Rule
Add a VLAN that requires translational bridging (values are not set to zero).	The translational bridging VLAN IDs that are used must already exist in the database. The translational bridging VLAN IDs that a configuration points to must also contain a pointer to the original VLAN in one of the translational bridging parameters (for example, Ethernet points to FDDI, and FDDI points to Ethernet). The translational bridging VLAN IDs that a configuration points to must be different media types than the original VLAN (for example, Ethernet can point to Token Ring). If both translational bridging VLAN IDs are configured, these VLANs must be different media types (for example, Ethernet can point to FDDI and Token Ring).

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of VLAN *xxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default said-value is 100000 plus the VLAN ID; the mtu-size variable is 1500; the stp-type is ieee. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter VLAN configuration mode:

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

This example shows how to create a VLAN group.

```
Device(config)#  vlan group xyz vlan-list 50-60
```

This example shows how to remove a VLAN group.

```
Device(config)#  no vlan group xyz vlan-list 50-60
```

This example shows how to remove a single VLAN from the VLAN group.

```
Device(config)#    no vlan group xyz vlan-list 51
```

This example shows how to remove multiple VLANs from the VLAN group.

```
Device(config)#    no vlan group xyz vlan-list 52-55
```

This example shows how to remove both single and multiple VLANs from the VLAN group.

```
Device(config)#    no vlan group xyz vlan-list 56, 58-60
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

vlan dot1q tag native

no vlan dot1q tag native

Note This command is not supported on devices running the LAN Base image.

Syntax Description This command has no arguments or keywords.

Command Default The IEEE 802.1Q native VLAN tagging is disabled.

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines When enabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are not tagged.

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the **vtp** command in global configuration mode. To remove the settings or to return to the default settings, use the **no** form of this command.

vtp {**domain** *domain-name*| **file** *filename*| **interface** *interface-name* [**only**]| **mode** {**client**| **off**| **server**| **transparent**} [**mst**| **unknown**| **vlan**]| **password** *password* [**hidden**| **secret**]| **pruning**| **version** *number*}

no vtp {**file**| **interface**| **mode** [**client**| **off**| **server**| **transparent**] [**mst**| **unknown**| **vlan**]| **password**| **pruning**| **version**}

Syntax Description

domain *domain-name*	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the device. The domain name is case sensitive.
file *filename*	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface *interface-name*	Specifies the name of the interface providing the VTP ID updated for this device.
only	(Optional) Uses only the IP address of this interface as the VTP IP updater.
mode	Specifies the VTP device mode as client, server, or transparent.
client	Places the device in VTP client mode. A device in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on a VTP client. VLANs are configured on another device in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.
off	Places the device in VTP off mode. A device in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.
server	Places the device in VTP server mode. A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the device. The device can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the device in VTP transparent mode. A device in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the device running configuration file, and you can save them in the device startup configuration file by entering the **copy running-config startup config** privileged EXEC command.
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).
unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).

password *password*	Sets the administrative domain password for the generation of the 16-byte secret value used in MD5 digest calculation to be sent in VTP advertisements and to validate received VTP advertisements. The password can be an ASCII string from 1 to 32 characters. The password is case sensitive.
hidden	(Optional) Specifies that the key generated from the password string is saved in the VLAN database file. When the **hidden** keyword is not specified, the password string is saved in clear text. When the hidden password is entered, you need to reenter the password to issue a command in the domain. This keyword is supported only in VTP Version 3.
secret	(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).
pruning	Enables VTP pruning on the device.
version *number*	Sets the VTP Version to Version 1, Version 2, or Version 3.

Command Default

The default filename is *flash:vlan.dat*.

The default mode is server mode and the default database is VLAN.

In VTP Version 3, for the MST database, the default mode is transparent.

No domain name or password is defined.

No password is configured.

Pruning is disabled.

The default version is Version 1.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you save VTP mode, domain name, and VLAN configurations in the device startup configuration file and reboot the device, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the device is not in client or transparent mode.
- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in transparent mode, the device configuration is not changed.
- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.
- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.
- In VTP Versions 1 and 2, the VTP mode must be transparent for VTP and VLAN information to be saved in the running configuration file.
- With VTP Versions 1 and 2, you cannot change the VTP mode to client or server if extended-range VLANs are configured on the switch. Changing the VTP mode is allowed with extended VLANs in VTP Version 3.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.
- When you use the **no vtp password** form of the command, the device returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Device(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Device(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Device(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the device:

```
Device(config)# vtp domain OurDomainName
```

This example shows how to place the device in VTP transparent mode:

```
Device(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Device(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Device(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on the interface, use the **no** form of this command.

vtp

no vtp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Enter this command only on interfaces that are in trunking mode.

This command is supported only when the device is running VTP Version 3.

This example shows how to enable VTP on an interface:

```
Device(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Device(config-if)# no vtp
```

vtp primary

To configure a device as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** command in privileged EXEC mode.

vtp primary [**mst**| **vlan**] **[force]**

Syntax Description

mst	(Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature.
vlan	(Optional) Configures the device as the primary VTP server for VLANs.
force	(Optional) Configures the device to not check for conflicting devices when configuring the primary server.

Command Default

The device is a VTP secondary server.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.

Note This command is supported only when the device is running VTP Version 3.

This example shows how to configure the device as the primary VTP server for VLANs:

```
Device# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

wireless broadcast vlan

To enable broadcast support on a VLAN, use the **wireless broadcast vlan** command in global configuration mode. To disable Ethernet broadcast support, use the **no** form of the command.

wireless broadcast vlan [*vlan-id*]

no wireless broadcast vlan [*vlan-id*]

Syntax Description

vlan-id	(Optional) Specifies the VLAN ID to enable broadcast support to that VLAN. The value ranges from 1 to 4095.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command in the global configuration mode only.

This example shows how to enable broadcasting on VLAN 20:

```
Device(config)# wireless broadcast vlan 20
```

PART XVII

WLAN

- WLAN Commands, page 975

CHAPTER 19

WLAN Commands

- aaa-override, page 976
- accounting-list, page 977
- assisted-roaming, page 978
- band-select, page 979
- broadcast-ssid, page 980
- call-snoop, page 981
- channel-scan defer-priority, page 982
- channel-scan defer-time, page 983
- chd, page 984
- client association limit, page 985
- client vlan, page 986
- ccx aironet-iesupport, page 987
- datalink flow monitor, page 988
- device-classification, page 989
- default, page 990
- dtim dot11, page 992
- exclusionlist, page 993
- exit, page 994
- exit (WLAN AP Group), page 994
- ip access-group, page 995
- ip flow monitor, page 996
- ip verify source mac-check, page 997
- load-balance, page 998
- mobility anchor, page 999

- nac, page 1000
- passive-client, page 1001
- peer-blocking, page 1002
- radio, page 1003
- radio-policy, page 1004
- roamed-voice-client re-anchor, page 1005
- security ft, page 1006
- security pmf, page 1007
- security web-auth, page 1008
- security wpa akm, page 1009
- service-policy (WLAN), page 1010
- session-timeout, page 1011
- show wlan, page 1012
- show wireless wlan summary, page 1014
- shutdown, page 1015
- sip-cac, page 1016
- static-ip tunneling, page 1017
- vlan, page 1018
- universal-admin, page 1018
- wgb non-cisco, page 1019
- wifidirect policy, page 1020
- wlan (AP Group Configuration), page 1021
- wlan, page 1022
- wlan shutdown, page 1023
- wmm, page 1023

aaa-override

To enable AAA override on the WLAN, use the **aaa-override** command. To disable AAA override, use the **no** form of this command.

aaa-override

no aaa-override

Syntax Description

This command has no keywords or arguments.

Command Default AAA is disabled by default.

Command Modes WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no aaa-override
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

accounting-list

To configure RADIUS accounting servers on a WLAN, use the **accounting-list** command. To disable RADIUS server accounting, use the **no** form of this command.

accounting-list *radius-server-acct*

no accounting-list

Syntax Description

radius-server-acct	Accounting RADIUS server name.

Command Default RADIUS server accounting is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure RADIUS server accounting on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# accounting-list test
Device(config-wlan)# end
```

This example shows how to disable RADIUS server accounting on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no accounting-list test
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

assisted-roaming

To configure assisted roaming using 802.11k on a WLAN, use the **assisted-roaming** command. To disable assisted roaming, use the **no** form of this command.

assisted-roaming {**dual-list**| **neighbor-list**| **prediction**}

no assisted-roaming {**dual-list**| **neighbor-list**| **prediction**}

Syntax Description

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.
neighbor-list	Configures an 802.11k neighbor list for a WLAN.
prediction	Configures assisted roaming optimization prediction for a WLAN.

Command Default

Neighbor list and dual band support are enabled by default. The default is the band that the client is currently associated with.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

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. To make changes to the WLAN, the WLAN must be in disabled state.

Example

The following example shows how to configure a 802.11k neighbor list on a WLAN:

```
Device(config-wlan)#assisted-roaming neighbor-list
```

The following example shows the warning message when load balancing is enabled on a WLAN. Load balancing must be disabled if it is already enabled when configuring assisted roaming:

```
Device(config)#wlan test-prediction 2 test-prediction
Device(config-wlan)#client vlan 43
Device(config-wlan)#no security wpa
Device(config-wlan)#load-balance
Device(config-wlan)#assisted-roaming prediction
WARNING: Enabling neighbor list prediction optimization may slow association and impact
VOICE client perform.
Are you sure you want to continue? (y/n)[y]: y
% Request aborted - Must first disable Load Balancing before enabling Assisted Roaming
Prediction Optimization on this WLAN.
```

band-select

To configure band selection on a WLAN, use the **band-select** command. To disable band selection, use the **no** form of this command.

band-select

no band-select

Syntax Description

This command has no keywords or arguments.

Command Default

Band selection is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When you enable band select on a WLAN, the access point suppresses client probes on 2.4GHz 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.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable band select on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# band-select
Device(config-wlan)# end
```

This example shows how to disable band selection on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no band-select
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

broadcast-ssid

To enable a Service Set Identifier (SSID) on a WLAN, use the **broadcast-ssid** command. To disable broadcasting of SSID, use the **no** form of this command.

broadcast-ssid

no broadcast-ssid

Syntax Description

This command has no keywords or arguments.

Command Default

The SSIDs of WLANs are broadcasted by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a broadcast SSID on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# broadcast-ssid
Device(config-wlan)# end
```

This example shows how to disable a broadcast SSID on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no broadcast-ssid
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

call-snoop

To enable Voice over IP (VoIP) snooping on a WLAN, use the **call-snoop** command. To disable Voice over IP (VoIP), use the **no** form of this command.

call-snoop

no call-snoop

Syntax Description

This command has no keywords or arguments.

Command Default

VoIP snooping is disabled by default.

Command Modes

WLN configuration

Usage Guidelines

You must disable the WLAN before using this command. See the Related Commands section for more information on how to disable a WLAN.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN on which call snooping is configured must be configured with Platinum QoS. You must disable quality of service before using this command. See Related Commands section for more information on configuring QoS service-policy.

This example shows how to enable VoIP on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# call-snoop
Device(config-wlan)# end
```

This example shows how to disable VoIP on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no call-snoop
Device(config-wlan)# end
```

Related Topics

service-policy (WLAN), on page 605

wlan, on page 1022

channel-scan defer-priority

To configure the device to defer priority markings for packets that can defer off-channel scanning, use the **channel-scan defer-priority** command. To disable the device to defer priority markings for packets that can defer off-channel scanning, use the **no** form of this command.

channel-scan defer-priority *priority*

no channel-scan defer-priority *priority*

Syntax Description

priority	Channel priority value. The range is 0 to 7. The default is 3.

Command Default

Channel scan defer is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable channel scan defer priority on a WLAN and set it to a priority value 4:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# channel-scan defer-priority 4
Device(config-wlan)# end
```

This example shows how to disable channel scan defer priority on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no channel-scan defer-priority 4
Device(config-wlan)# end
```

channel-scan defer-time

To assign a channel scan defer time, use the **channel-scan defer-time** command. To disable the channel scan defer time, use the **no** form of this command.

channel-scan defer-time *msecs*

no channel-scan defer-time

Syntax Description

msecs	Deferral time in milliseconds. The range is from 0 to 60000. The default is 100.

Command Default

Channel-scan defer time is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The time value in milliseconds should match the requirements of the equipment on the WLAN.

This example shows how to enable a channel scan on the WLAN and set the scan deferral time to 300 milliseconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# channel-scan defer-time 300
Device(config-wlan)# end
```

This example shows how to disable channel scan defer time on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no channel-scan defer-time
Device(config-wlan)# end
```

chd

To enable coverage hole detection on a WLAN, use the **chd** command. To disable coverage hole detection, use the **no** form of this command.

chd

no chd

Syntax Description

This command has no keywords or arguments.

Command Default

Coverage hole detection is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable coverage hole detection on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# chd
Device(config-wlan)# end
```

This example shows how to disable coverage hole detection on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no chd
Device(config-wlan)# end
```

client association limit

To configure the maximum number of client connections, clients per access points, or clients per access point radio on a WLAN, use the **client association limit** command. To disable clients association limit on the WLAN, use the **no** form of this command.

client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

no client association limit {*association-limit*| **ap** *ap-limit*| **radio** *max-ap-radio-limit*}

Syntax Description

association-limit	Number of client connections to be accepted. The range is from 0 to 2000. A value of zero (0) indicates no set limit.
ap	Maximum number of clients per access point.
ap-limit	Configures the maximum number of client connections to be accepted per access point radio. The valid range is from 0 to 400.
radio	Configures the maximum number of clients per AP radio.
max-ap-radio-limit	Maximum number of client connections to be accepted per access point radio. The valid range is from 0 - 200.

Command Default

The maximum number of client connections is set to 0 (no limit).

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The command was modified. The **ap** and **radio** keywords were added.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client association limit on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# client association limit 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no client association limit
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per radio on a WLAN and configure the client limit to 200:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit radio 200
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

This example shows how to configure a client association limit per AP on a WLAN and configure the client limit to 300::

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client association limit ap 300
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

client vlan

To configure a WLAN interface or an interface group, use the **client vlan** command. To disable the WLAN interface, use the **no** form of this command.

client vlan *interface-id-name-or-group-name*

no client vlan

Syntax Description

interface-id-name-or-group-name	Interface ID, name, or VLAN group name. The interface ID can also be in digits too.

Command Default The default interface is configured.

Command Modes WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# client vlan client-vlan1
Device(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no client vlan
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

ccx aironet-iesupport

To enable Aironet Information Elements (IEs) for a WLAN, use the **ccx aironet-iesupport** command. To disable Aironet Information Elements (IEs), use the **no** form of this command.

ccx aironet-iesupport

no ccx aironet-iesupport

Syntax Description This command has no keywords or arguments.

Command Default Aironet IE support is enabled.

Command Modes WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable an Aironet IE for a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ccx aironet-iesupport
Device(config-wlan)# end
```

This example shows how to disable an Aironet IE on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ccx aironet-iesupport
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

datalink flow monitor

To enable NetFlow monitoring in a WLAN, use the **datalink flow monitor** command. To disable NetFlow monitoring, use the **no** form of this command.

datalink flow monitor *datalink-monitor-name* {**input**| **output**}

no datalink flow monitor *datalink-monitor-name* {**input**| **output**}

Syntax Description

datalink-monitor-name	Flow monitor name. The datalink monitor name can have up to 31 characters.
input	Specifies the NetFlow monitor for ingress traffic.
output	Specifies the NetFlow monitor for egress traffic.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable NetFlow monitoring on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# datalink flow monitor test output
Device(config-wlan)# end
```

This example shows how to disable NetFlow monitoring on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no datalink flow monitor test output
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

device-classification

To enable client device classification in a WLAN, use the **device-classification** command. To disable device classification, use the **no** form of this command.

device-classification

no device-classification

Syntax Description

device-classification	Enables/Disables Client Device Classification.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# device-classification
Device(config-wlan)# end
```

default

To set the parameters to their default values, use the **default** command.

default {**aaa-override**| **accounting-list**| **band-select**| **broadcast-ssid**| **call-snoop**| **ccx**| **channel-scan**| **parameters**| **chd**| **client**| **datalink**| **diag-channel**| **dtim**| **exclusionlist**| **ip**| **ipv6**| **load-balance**| **local-auth**| **mac-filtering**| **media-stream**| **mfp**| **mobility**| **nac**| **passive-client**| **peer-blocking**| **radio**| **roamed-voice-client**| **security**| **service-policy**| **session-timeout**| **shutdown**| **sip-cac**| **static-ip**| **uapsd**| **wgb**| **wmm**}

Syntax Description

aaa-override	Sets the AAA override parameter to its default value.
accounting-list	Sets the accounting parameter and its attributes to their default values.
band-select	Sets the band selection parameter to its default values.
broadcast-ssid	Sets the broadcast Service Set Identifier (SSID) parameter to its default value.
call-snoop	Sets the call snoop parameter to its default value.
ccx	Sets the Cisco client extension (Cisco Aironet IE) parameters and attributes to their default values.
channel-scan	Sets the channel scan parameters and attributes to their default values.
chd	Sets the coverage hold detection parameter to its default value.
client	Sets the client parameters and attributes to their default values.
datalink	Sets the datalink parameters and attributes to their default values.
diag-channel	Sets the diagnostic channel parameters and attributes to their default values.
dtim	Sets the Delivery Traffic Indicator Message (DTIM) parameter to its default value.
exclusionlist	Sets the client exclusion timeout parameter to its default value.
ip	Sets the IP parameters to their default values.
ipv6	Sets the IPv6 parameters and attributes to their default values.

load-balance	Sets the load-balancing parameter to its default value.
local-auth	Sets the Extensible Authentication Protocol (EAP) profile parameters and attributes to their default values.
mac-filtering	Sets the MAC filtering parameters and attributes to their default values.
media-stream	Sets the media stream parameters and attributes to their default values.
mfp	Sets the Management Frame Protection (MPF) parameters and attributes to their default values.
mobility	Sets the mobility parameters and attributes to their default values.
nac	Sets the RADIUS Network Admission Control (NAC) parameter to its default value.
passive-client	Sets the passive client parameter to its default value.
peer-blocking	Sets the peer to peer blocking parameters and attributes to their default values.
radio	Sets the radio policy parameters and attributes to their default values.
roamed-voice-client	Sets the roamed voice client parameters and attributes to their default values.
security	Sets the security policy parameters and attributes to their default values.
service-policy	Sets the WLAN quality of service (QoS) policy parameters and attributes to their default values.
session-timeout	Sets the client session timeout parameter to its default value.
shutdown	Sets the shutdown parameter to its default value.
sip-cac	Sets the Session Initiation Protocol (SIP) Call Admission Control (CAC) parameters and attributes to their default values.
static-ip	Sets the static IP client tunneling parameters and their attributes to their default values.
uapsd	Sets the Wi-Fi Multimedia (WMM) Unscheduled Automatic Power Save Delivery (UAPSD) parameters and attributes to their default values.
wgb	Sets the Workgroup Bridges (WGB) parameter to its default value.
wmm	Sets the WMM parameters and attributes to their default values.

Command Default

None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to set the Cisco Client Extension parameter to its default value:

```
Device(config-wlan)# default ccx aironet-iesupport
```

Related Topics

wlan, on page 1022

dtim dot11

To configure the Delivery Traffic Indicator Message (DTIM) period for a WLAN, use the **dtim dot11** command. To disable DTIM, use the **no** form of this command.

dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

no dtim dot11 {**5ghz**| **24ghz**} *dtim-period*

Syntax Description

5ghz	Configures the DTIM period on the 5-GHz band.
24ghz	Configures the DTIM period on the 2.4-GHz band.
dtim-period	Value for the DTIM period. The range is from 1 to 255.

Command Default

The DTIM period is set to 1.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the DTIM period on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# dtim dot11 24ghz 3
```

This example shows how to disable the DTIM period on a WLAN on the 2.4-GHz band:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no dtim dot11 24ghz 3
```

Related Topics

wlan, on page 1022

exclusionlist

To configure an exclusion list on a wireless LAN, use the **exclusionlist** command. To disable an exclusion list, use the **no** form of this command.

exclusionlist [**timeout** *seconds*]

no exclusionlist [timeout]

Syntax Description

timeout *seconds*	(Optional) Specifies an exclusion list timeout in seconds. The range is from 0 to 2147483647. A value of zero (0) specifies no timeout.

Command Default

The exclusion list is set to 60 seconds.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure a client exclusion list for a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no exclusionlist timeout 345
```

exit

To exit the WLAN configuration submode, use the **exit** command.

exit

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to exit the WLAN configuration submode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# exit
Device(config)#
```

exit (WLAN AP Group)

To exit the WLAN access point group submode, use the **exit** command.

exit

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to exit the WLAN AP group submode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group test
Device(config-apgroup)# exit
```

ip access-group

To configure WLAN access control group (ACL), use the **ip access-group** command. To remove a WLAN ACL group, use the **no** form of the command.

ip access-group [web] *acl-name*

no ip access-group [web]

Syntax Description

web	(Optional) Configures the IPv4 web ACL.
acl-name	Specify the preauth ACL used for the WLAN with the security type value as webauth.

Command Default None

Command Modes WLAN configuration

Usage Guidelines You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a WLAN ACL:

```
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip access-group web test
Device(config-wlan)#
```

Related Topics

wlan, on page 1022

ip flow monitor

To configure IP NetFlow monitoring, use the **ip flow monitor** command. To remove IP NetFlow monitoring, use the **no** form of this command.

ip flow monitor *ip-monitor-name* {**input**| **output**}

no ip flow monitor *ip-monitor-name* {**input**| **output**}

Syntax Description

ip-monitor-name	Flow monitor name.
input	Enables a flow monitor for ingress traffic.
output	Enables a flow monitor for egress traffic.

Command Default

None

Command Modes

WLAN configuration

Usage Guidelines

You must disable the WLAN before using this command.

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure an IP flow monitor for the ingress traffic:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip flow monitor test input
```

ip verify source mac-check

To enable IPv4 Source Guard (IPSG) on a WLAN, use the **ip verify source mac-check** command. To disable IPSG, use the **no** form of this command.

ip verify source mac-check

no ip verify source mac-check

Syntax Description

This command has no keywords or arguments.

Command Default

IPSG is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this feature to restrict traffic from a host to a specific interface that is based on the host's IP address. The feature can also be configured to bind the source MAC and IP of a host so that IP spoofing is prevented.

Use this feature to bind the IP and MAC address of a wireless host that is based on information received from DHCP snooping, ARP, and Dataglean. Dataglean is the process of extracting location information such as host hardware address, ports that lead to the host, and so on from DHCP messages as they are forwarded by the DHCP relay agent. If a wireless host tries to send traffic with IP address and MAC address combination

that has not been learned by the device, this traffic is dropped in the hardware. IPSG is not supported on DHCP packets. IPSG is not supported for foreign clients in a foreign device.

You must disable the WLAN before using this command.

This example shows how to enable IPSG:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# ip verify source mac-check
```

This example shows how to disable IPSG:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no ip verify source mac-check
```

load-balance

To enable load balancing on a WLAN, use the **load-balance** command. To disable load balancing, use the **no** form of this command.

load-balance

no load-balance

Syntax Description

This command has no keywords or arguments.

Command Default

Load balancing is disabled by default.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	The command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable load balancing on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# shutdown
Device(config)# wlan wlan1
Device(config-wlan)# load-balance
Device(config)# no shutdown
Device(config-wlan)# end
```

This example shows how to disable load balancing on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# shutdown
Device(config)# wlan wlan1
Device(config-wlan)# no load-balance
Device(config)# no shutdown
Device(config-wlan)# end
```

Related Topics

wlan, on page 1022

mobility anchor

To configure mobility sticky anchoring, use the **mobility anchor sticky** command. To disable the sticky anchoring, use the **no** form of the command.

To configure guest anchoring, use the **mobility anchor** *ip-address* command.

To delete the guest anchor, use the **no** form of the command.

To configure the device as an auto-anchor, use the **mobility anchor** command.

mobility anchor {*ip-address*| **sticky**}

no mobility anchor {*ip-address*| **sticky**}

Syntax Description

sticky	The client is anchored to the first switch that it associates. **Note** This command is by default enabled and ensures low roaming latency. This ensures that the point of presence for the client does not change when the client joins the mobility domain and roams within the domain.
ip-address	Configures the IP address for the guest anchor device to this WLAN.

Command Default

Sticky configuration is enabled by default.

Command Modes

WLAN Configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.
Cisco IOS XE 3.3SE	The auto-anchor configuration required the device IP address to be entered prior to the Cisco IOS XE 3.3SE release; with this release, if no IP address is given, the device itself becomes an anchor; you do not have to explicitly specify the IP address.

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.
- Mobility uses the following ports, that are allowed through the firewall:
  - 16666
  - 16667
  - 16668

This example shows how to enable the sticky mobility anchor:

```
Device(config-wlan)# mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Device(config-wlan)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Device(config-wlan)# mobility anchor
```

nac

To enable RADIUS Network Admission Control (NAC) support for a WLAN, use the **nac** command. To disable NAC out-of-band support, use the **no** form of this command.

nac

no nac

Syntax Description

This command has no keywords or arguments.

Command Default

NAC is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You should enable AAA override before you enable the RADIUS NAC state.

This example shows how to configure RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# aaa-override
Device(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no nac
Device(config-wlan)# no aaa-override
```

Related Topics

aaa-override, on page 976

passive-client

To enable the passive client feature on a WLAN, use the **passive-client** command. To disable the passive client feature, use the **no** form of this command.

passive-client

no passive-client

Syntax Description

This command has no keywords or arguments.

Command Default

Passive client feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must enable the global multicast mode and multicast-multicast mode before entering this command. Both multicast-multicast mode and multicast unicast modes are supported. The multicast-multicast mode is recommended.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This show how to enable the passive client feature on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
```

```
Device(config)# wlan test-wlan
Device(config-wlan)# passive-client
```

This example shows how to disable the passive client feature on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wireless multicast
Device(config)# wlan test-wlan
Device(config-wlan)# no passive-client
```

Related Topics

wlan, on page 1022

peer-blocking

To configure peer-to-peer blocking on a WLAN, use the **peer-blocking** command. To disable peer-to-peer blocking, use the **no** form of this command.

peer-blocking {**drop**| **forward-upstream**}

no peer-blocking

Syntax Description

drop	Specifies the device to discard the packets.
forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the device decides what action to take regarding the packets.

Command Default

Peer blocking is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# peer-blocking  drop
Device(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no peer-blocking  drop
Device(config-wlan)# no peer-blocking forward-upstream
```

Related Topics

wlan, on page 1022

radio

To enable the Cisco radio policy on a WLAN, use the **radio** command. To disable the Cisco radio policy on a WLAN, use the **no** form of this command.

radio {**all**| **dot11a**| **dot11ag**| **dot11bg**| **dot11g**}

no radio

Syntax Description

all	Configures the WLAN on all radio bands.
dot11a	Configures the WLAN on only 802.11a radio bands.
dot11ag	Configures the WLAN on 802.11a/g radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g radio bands (only 802.11b if 802.11g is disabled).
dot11g	Configures the wireless LAN on 802.11g radio bands only.

Command Default

Radio policy is enabled on all bands.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure the WLAN on all radio bands:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# wlan wlan1
Device(config-wlan)# radio all
```

This example shows how to disable all radio bands on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no radio all
```

Related Topics

wlan, on page 1022

radio-policy

To configure the radio policy on a WLAN access point group, use the **radio-policy** command. To disable the radio policy on the WLAN, use the **no** form of this command.

radio-policy {**all**| **dot11a**| **dot11bg**| **dot11g**}

no radio{**all**| **dot11a**| **dot11bg**| **dot11g**}

Syntax Description

all	Configures the wireless LAN on all radio bands.
dot11a	Configures the wireless LAN on only 802.11a radio bands.
dot11bg	Configures the wireless LAN on only 802.11b/g (only 802.11b if 802.11g is disabled) radio bands.
dot11g	Configures the wireless LAN on only 802.11g radio bands.

Command Default

Radio policy is enabled on all the bands.

Command Modes

WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The WLAN must be restarted for the changes to take effect. See Related Commands section for more information on how to shutdown a WLAN.

This example shows how to enable the radio policy on the 802.11b band for an AP group:

```
Device(config)# ap group test
Device(config-apgroup)# wlan test-wlan
```

```
Device(config-wlan-apgroup)# radio-policy dot11b
```

This example shows how to disable the radio policy on the 802.11b band of an AP group:

```
Device(config)# ap group test
Device(config-apgroup)# wlan test-wlan
Device(config-wlan-apgroup)# no radio-policy dot11bg
```

Related Topics

wlan, on page 1022

wlan shutdown, on page 1023

roamed-voice-client re-anchor

To enable the roamed-voice-client re-anchor feature, use the **roamed-voice-client re-anchor** command. To disable the roamed-voice-client re-anchor feature, use the **no** form of this command.

roamed-voice-client re-anchor

no roamed-voice-client re-anchor

Syntax Description

This command has no keywords or arguments.

Command Default

Roamed voice client reanchor feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable the roamed voice client re-anchor feature:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# roamed-voice-client re-anchor
```

This example shows how to disable the roamed voice client re-anchor feature:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no roamed-voice-client re-anchor
```

Related Topics

wlan, on page 1022

security ft

To configure 802.11r fast transition parameters, use the **security ft** command. To configure fast transition **over the air**, use the **no security ft over-the-ds** command.

security ft [**over-the-ds**| **reassociation-timeout** *timeout-jn-seconds*]

no security ft [**over-the-ds**| **reassociation-timeout**]

Syntax Description

over-the-ds	(Optional) Specifies that the 802.11r fast transition occurs over a distributed system. The no form of the command with this parameter configures security ft over the air.
reassociation-timeout	(Optional) Configures the reassociation timeout interval.
timeout-in-seconds	(Optional) Specifies the reassociation timeout interval in seconds. The valid range is between 1 to 100. The default value is 20.

Command Default

The feature is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

None

WLAN Security must be enabled.

Example

The following example configures security FT configuration for an open WLAN:

```
Device#wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no mobility anchor sticky
Device(config-wlan)# no security wpa
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# no security wpa wpa2
Device(config-wlan)# no security wpa wpa2 ciphers aes
```

```
Device(config-wlan)# security ft
Device(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Device# wlan test
Device(config-wlan)# client vlan 0140
Device(config-wlan)# no security wpa akm dot1x
Device(config-wlan)# security wpa akm ft psk
Device(config-wlan)# security wpa akm psk set-key ascii 0 test-test
Device(config-wlan)# security ft
Device(config-wlan)# no shutdown
```

security pmf

To configure 802.11w Management Frame Protection (PMF) on a WLAN, use the **security pmf** command. To disable management frame protection, use the **no** form of the command.

security pmf {**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*}

no security pmf [**association-comeback** *association-comeback-time-seconds*| **mandatory**| **optional**| **saquery-retry-time** *saquery-retry-time-milliseconds*]

Syntax Description

association-comeback	Configures the 802.11w association comeback time.
association-comeback-time-seconds	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 through 20 seconds.
mandatory	Specifies that clients are required to negotiate 802.1w PMF protection on the WLAN.
optional	Specifies that the WLAN does not mandate 802.11w support on clients. Clients with no 802.11w capability can also join.
saquery-retry-time	Time interval identified before which the SA query response is expected. If the device does not get a response, another SA query is tried.
saquery-retry-time-milliseconds	The saquery retry time in milliseconds. The range is from 100 to 500 ms. The value must be specified in multiples of 100 milliseconds.

Command Default

PMF is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

You must have WPA (Wi-Fi Protected Access) and AKM (Authentication Key Management) configured to use this feature. See Related Command section for more information on configuring the security parameters.

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 (device) 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 WPA2 security at Layer 2.

This example shows how to enable the association comeback value at 15 seconds.

```
Device(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Device(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Device(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Device(config-wlan)# no security pmf
```

Related Topics

security wpa akm, on page 1009

security web-auth

To change the status of web authentication used on a WLAN, use the **security web-auth** command. To disable web authentication on a WLAN, use the **no** form of the command.

security web-auth [**authentication-list** *authentication-list-name*| **on-macfilter-failure**| **parameter-map** *parameter-map-name*]

no security web-auth [**authentication-list [authentication-list-name]| on-macfilter-failure**| **parameter-map [parameter-name]**]

Syntax Description

authentication-list *authentication-list-name*	Sets the authentication list for IEEE 802.1x.
on-macfilter-failure	Enables web authentication on MAC failure.

parameter-map *parameter-map-name*	Configures the parameter map.

Command Default

Web authentication is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Examples

The following example shows how to configure the authentication-list web authentication on a WLAN:

```
Device(config-wlan)# security web-auth authentication-list test
```

security wpa akm

To configure authentication key management using Cisco Centralized Key Management (CCKM), use the **security wpa akm** command. To disable the authentication key management for Cisco Centralized Key Management, use the **no** form of the command.

security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

no security wpa [**akm** {**cckm**| **dot1x**| **ft**| **pmf**| **psk**}| **wpa1** [**ciphers** {**aes**| **tkip**}]| **wpa2** [**ciphers** {**aes**| **tikp**}]]

Syntax Description

akm	Configures the Authentication Key Management (AKM) parameters.
aes	Configures AES (Advanced Encryption Standard) encryption support.
cckm	Configures Cisco Centralized Key Management support.
ciphers	Configures WPA ciphers.
dot1x	Configures 802.1x support.
ft	Configures fast transition using 802.11r.

pmf	Configures 802.11w management frame protection.
psk	Configures 802.11r fast transition pre-shared key (PSK) support.
tkip	Configures Temporal Key Integrity Protocol (TKIP) encryption support.
wpa2	Configures Wi-Fi Protected Access 2 (WPA2) support.

Command Default

By default Wi-Fi Protected Access2, 802.1x are enabled. WPA2, PSK, CCKM, FT dot1x, FT PSK, PMF dot1x, PMF PSK, FT Support are disabled. The FT Reassociation timeout is set to 20 seconds, PMF SA Query time is set to 200.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

The following example shows how to configure CCKM on the WLAN.

```
Device(config-wlan)#security wpa akm cckm
```

service-policy (WLAN)

To configure the WLAN quality of service (QoS) service policy, use the **service-policy** command. To disable a QoS policy on a WLAN, use the **no** form of this command.

service-policy [client] {**input**| **output**} *policy-name*

no service-policy [client] {**input**| **output**} *policy-name*

Syntax Description

client	(Optional) Assigns a policy map to all clients in the WLAN.
input	Assigns an input policy map.
output	Assigns an output policy map.

policy-name	The policy name.

Command Default

No policies are assigned and the state assigned to the policy is None.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no service-policy input policy-test
```

This example shows how to configure the output QoS service policy on a WLAN to platinum (precious metal policy):

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# service-policy output platinum
```

Related Topics

wlan, on page 1022

wlan, on page 1022

session-timeout

To configure session timeout for clients associated to a WLAN, use the **session-timeout** command. To disable a session timeout for clients that are associated to a WLAN, use the **no** form of this command.

session-timeout seconds

no session-timeout

Syntax Description

seconds	Timeout or session duration in seconds. A value of zero (0) is equivalent to no timeout. The range is from 300 to 86400.

Command Default

The client timeout is set to 1800 seconds for WLANs that are configured with dot1x security. The client timeout is set to 0 for open WLANs.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to configure a session timeout to 300 seconds:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no session-timeout
```

show wlan

To view WLAN parameters, use the **show wlan** command.

show wlan {**all** | **id** *wlan-id*| **name** *wlan-name* | **summary**}

Syntax Description

all	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
id *wlan-id*	Specifies the wireless LAN identifier. The range is from 1 to 512.
name *wlan-name*	Specifies the WLAN profile name. The name is from 1 to 32 characters.
summary	Displays a summary of the parameters configured on a WLAN.

Command Default None

Command Modes Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to display a summary of the WLANs configured on the device:

```
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                      SSID                            VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                   1    UP
```

This example shows how to display a summary of parameters configured on a particular WLAN:

```
Device# show wlan name test-wlan
WLAN Identifier                                 : 45
Profile Name                                    : test-wlan
Network Name (SSID)                             : test-wlan-ssid
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusionlist Timeout                           : 60
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : test
WLAN IPv4 ACL                                   : test
WLAN IPv6 ACL                                   : unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : ap-mac
DHCP Option 82 Ascii Mode                       : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WifiDirect                                      : Disabled
WMM                                             : Disabled
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
```

```
CCX - AironetIe Support                         : Enabled
CCX - Gratuitous ProbeResponse (GPR)            : Disabled
CCX - Diagnostics Channel Capability            : Disabled
Dot11-Phone Mode (7920)                         : Invalid
Wired Protocol                                  : None
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Enabled
            PSK                                 : Disabled
            CCKM                                : Disabled
    IP Security                                 : Disabled
    IP Security Passthru                        : Disabled
    L2TP                                        : Disabled
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Auto Anchor                                 : Disabled
    Sticky Anchoring                            : Enabled
    Cranite Passthru                            : Disabled
    Fortress Passthru                           : Disabled
    PPTP                                        : Disabled
    Infrastructure MFP protection               : Enabled
    Client MFP                                  : Optional
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
    Tkip MIC Countermeasure Hold-down Timer     : 60
Call Snooping                                   : Disabled
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
IP Source Guard                                 : Disabled
Netflow Monitor                                 : test
        Direction                               : Input
        Traffic                                 : Datalink

Mobility Anchor List
IP Address
-----------
```

show wireless wlan summary

To display wireless wlan summary, use the **show wireless wlan summary** command.

show wireless wlan summary

Syntax Description

This command has no keywords or arguments.

Command Default None

Command History

Release	Modification
15.2(3)E	This command was introduced.

The following is a sample output of the **show wireless wlan summary** command.

```
Cisco-Controller# show wireless wlan summary

Total WLAN Configured: 3

Total Client Count: 0


ID    Profile Name          SSID                 Security    Radio       VLAN        Client
   Status
-----------------------------------------------------------------------------------------------
1     Test1                 xxx                   WPA1/WPA2   All         1           0
     DOWN
2     wlan1                 wlan2-ssid            WPA1/WPA2   All         1           0
     DOWN
3     wlan3                 mywlan3               WPA1/WPA2   All         1           0
     DOWN
```

shutdown

To disable a WLAN, use the **shutdown** command. To enable a WLAN, use the **no** form of this command.

shutdown

no shutdown

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to disable a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan test-wlan
Device(config-wlan)# shutdown
Device(config-wlan)# end
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                  1    DOWN
```

This example shows how to enable a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan test-wlan
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan summary
Number of WLANs: 1

WLAN Profile Name                     SSID                           VLAN Status
-------------------------------------------------------------------------------
45   test-wlan                         test-wlan-ssid                  1    UP
```

sip-cac

To configure the Session Initiation Protocol (SIP) Call Admission Control (CAC) feature on a WLAN, use the **sip-cac** command. To disable the SIP CAC feature, use the **no** form of this command.

sip-cac {**disassoc-client**| **send-486busy**}

no sip-cac {**disassoc-client**| **send-486busy**}

Syntax Description

disassoc-client	Enables a client disassociation if a CAC failure occurs.
send-486busy	Sends a SIP 486 busy message if a CAC failure occurs.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable a client disassociation and 486 busy message on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# sip-cac disassoc-client
Device(config-wlan)# sip-cac send-486busy
```

This example shows how to disable a client association and 486 busy message on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no sip-cac disassoc-client
Device(config-wlan)# no sip-cac send-486busy
```

Related Topics

wlan, on page 1022

static-ip tunneling

To enable static IP tunneling on a WLAN, use the **static-ip tunneling** command. To disable the static IP tunneling feature, use the **no** form of this command.

static-ip tunneling

no static-ip tunneling

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to enable static-IP tunneling:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# static-ip tunneling
```

This example shows how to disable static-IP tunneling:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no static-ip tunneling
```

vlan

To assign a VLAN to an AP group, use the **vlan** command. To remove a VLAN ID, use the **no** form of this command.

vlan *interface-name*

no vlan

Syntax Description

interface-name	VLAN interface name.

Command Default

No VALN is assigned to the AP group. See Related Commands section for more information on how to disable a WLAN.

Command Modes

WLAN AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command.

This example shows how to configure a VLAN on an AP group:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group ap-group-1
Device(config-apgroup)# wlan test-wlan
Device(config-wlan-apgroup)# vlan 3
```

Related Topics

wlan, on page 1022

universal-admin

To configure the WLAN as the universal admin, use the **universal-admin** command. To remove the configuration, use the **no** form of this command.

universal-admin

Command Default

None

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.7.0 E	This command was introduced.

```
Deviceenable
Device#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)#wlan wlan1
Device(config-wlan)#universal-admin
```

wgb non-cisco

To enable non-Cisco Workgroup Bridges (WGB) clients on the WLAN, use the **wgb non-cisco** command. To disable support for non-Cisco WGB clients, use the **no** form of this command.

wgb non-cisco

no wgb non-cisco

Syntax Description

This command has no keywords or arguments.

Command Default

Non-Cisco WGB clients are disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable non-Cisco WGBs on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# wgb non-cisco
Device(config-wlan)# no shutdown
```

This example shows how to disable support for non-Cisco WGB clients on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
Device(config-wlan)# no wgb non-cisco
Device(config-wlan)# no shutdown
```

wifidirect policy

To configure Wi-Fi Direct client policy on a WLAN, use the **wifidirect policy** command. To disable Wi-Fi Direct Client policy, use the **no** form of the command.

wifidirect policy {**permit**| **deny**}

Syntax Description

permit	Enables Wi-Fi Direct clients to associate with the WLAN.
deny	When the Wi-Fi Direct policy is configured as "deny", the device permits or denies Wi-Fi Direct devices based on the device capabilities. A WI-Fi Direct device reports these capabilities in its association request to the device and these are based on the Wi-Fi capabilities of the device. These include: • Concurrent Operation • Cross connection If the Wi-Fi device supports either concurrent operations or cross connections or both, the client association is denied. The client can associate if the device does not support concurrent operations and cross connections.

Command Default

Wi-Fi Direct is disabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.3SE	This command was introduced.

Example

The following example shows how to enable Wi-Fi Direct and configure the Wi-Fi Direct clients to associate with the WLAN:

```
Device(config-wlan)# wifidirect policy permit
```

wlan (AP Group Configuration)

To configure WLAN parameters of a WLAN in an access point (AP) group, use the **wlan** command. To remove a WLAN from the AP group, use the **no** form of this command.

wlan *wlan-name*

no wlan *wlan-name*

Syntax Description

wlan-name	WLAN profile name. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN parameters are not configured for an AP group.

Command Modes

AP Group configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to configure WLAN related parameters in the AP group configuration mode:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ap group test
Device(config-apgroup)# wlan qos-wlan
```

Related Topics

wlan, on page 1022

wlan

To create a wireless LAN, use the **wlan** command. To disable a wireless LAN, use the **no** form of this command.

wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

no wlan [*wlan-name*| *wlan-name wlan-id*| *wlan-name wlan-id wlan-ssid*]

Syntax Description

wlan-name	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
wlan-id	Wireless LAN identifier. The range is from 1 to 512.
wlan-ssid	SSID. The range is from 1 to 32 alphanumeric characters.

Command Default

WLAN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

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 (Access Point 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.

This example shows how to create a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config)# no wlan test-wlan-cr 67 test-wlan-cr-ssid
```

wlan shutdown

To disable a WLAN, use the **wlan shutdown** command. To enable a WLAN, use the **no** form of this command.

wlan shutdown

no wlan shutdown

Command Default

The WLAN is disabled.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to shut down a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# shutdown
```

Related Topics

wlan, on page 1022

wmm

To enable Wi-Fi Multimedia (WMM) on a WLAN, use the **wmm** command. To disable WMM on a WLAN, use the **no** form of this command.

wmm {**allowed**| **require**}

no wmm

Syntax Description

allowed	Allows WMM on a WLAN.
require	Mandates that clients use WMM on the WLAN.

Command Default

WMM is enabled.

Command Modes

WLAN configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When the device 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 device.

You must disable the WLAN before using this command. See Related Commands section for more information on how to disable a WLAN.

This example shows how to enable WMM on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# wmm allowed
```

This example shows how to disable WMM on a WLAN:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# wlan wlan1
Device(config-wlan)# no wmm
```

Related Topics

wlan, on page 1022

INDEX

A

aaa-override command 976
access-session mac-move deny command 667
accounting-list command 977
action command 669
ap auth-list ap-policy 341
ap bridging 341
ap capwap multicast 342
ap capwap retransmit 343
ap capwap timers 344
ap cdp 345
ap core-dump 346
ap country 347
ap crash-file 348
ap dot11 2.4 GHz CleanAir alarm device 27
ap dot11 24ghz 349
ap dot11 24ghz cleanair 20
ap dot11 24ghz cleanair command 19, 21, 29
ap dot11 24ghz dot11g 349
ap dot11 24ghz or 5ghz rrm channel dca add command 640
ap dot11 24ghz or 5ghz rrm channel dca remove number 641
ap dot11 24ghz rrm coverage command 642
ap dot11 5ghz channelswitch mode 350
ap dot11 5ghz cleanair 14
ap dot11 5ghz cleanair command 15, 16, 25
ap dot11 5ghz power-constraint 351
ap dot11 5ghz rrm channel dca chan-width-11n 642
ap dot11 5ghz rrm channel device command 18
ap dot11 5ghz rrm command 635
ap dot11 5ghz rrm group-member command 644
ap dot11 5ghz rrm profile command 645
ap dot11 5ghz rrm tpc-threshold command 646
ap dot11 5ghz rrm txpower command 647
ap dot11 beaconperiod 352
ap dot11 beamforming 353
ap dot11 cac media-stream 354
ap dot11 cac video 357
ap dot11 cac voice 358
ap dot11 cleanair 361
ap dot11 cleanair alarm air-quality 362
ap dot11 cleanair alarm device 363
ap dot11 cleanair device 364
ap dot11 command 929
ap dot11 dot11n 365
ap dot11 dtpc 368
ap dot11 dual-band cleanair 406
ap dot11 edcs-parameters 369
ap dot11 l2roam rf-params 372
ap dot11 media-stream 373
ap dot11 multimedia 356
ap dot11 rrm ccx command 638
ap dot11 rrm ccx location-measurement 374
ap dot11 rrm channel cleanair-event 371
ap dot11 rrm channel command 17, 23, 638
ap dot11 rrm channel dca 375
ap dot11 rrm group-member 377
ap dot11 rrm group-mode 370
ap dot11 rrm logging 378
ap dot11 rrm monitor 379
ap dot11 rrm monitor mode command 644
ap dot11 rrm ndp-type 380
ap dot1x max-sessions 382
ap dot1x username 382
ap ethernet duplex 383
ap group 384
ap image 385
ap led 387
ap link-encryption 387
ap link-latency 388
ap mgmtuser username 388
ap name 49ghz rrm profile 400
ap name ap-groupname 390
ap name bhrate 391
ap name bridgegroupname 392
ap name bridging 393
ap name capwap retransmit 395
ap name command 396
ap name console-redirect 394
ap name core-dump 396
ap name country 397
ap name crash-file 398
ap name dot11 24ghz rrm coverage 399
ap name dot11 5ghz rrm channel 402

ap name dot11 antenna 402
ap name dot11 antenna extantgain 404
ap name dot11 cleanair 404
ap name dot11 dot11n antenna 405
ap name dot11 rrm ccx 407
ap name dot11 rrm profile 408
ap name dot11 txpower 410
ap name dot1xuser 411
ap name ethernet 412
ap name ethernet duplex 413
ap name image 414
ap name led 417
ap name link-encryption 418
ap name link-latency 418
ap name location 419
ap name mgmtuser 420
ap name mode 421
ap name monitor-mode 422
ap name monitor-mode dot11b 423
ap name name 424
ap name no cdp interface 393
ap name no dot11 shutdown 424
ap name no telnet 429
ap name power command 425
ap name power injector 429
ap name power pre-standard 430
ap name reset 431
ap name reset-button 431
ap name shutdown 426
ap name slot 432
ap name slot shutdown 426
ap name sniff 427
ap name ssh 428
ap name static-ip 433
ap name stats-timer 434
ap name syslog host 435
ap name syslog level 436
ap name tcp-adjust-mss 437
ap name tftp-downgrade 438
ap power injector 438
ap power pre-standard 439
ap reporting-period 440
ap reset-button 440
ap static-ip 442
ap syslog 442
ap tcp-adjust-mss size 445
ap tftp-downgrade 445
arp command 812
assisted-roaming command 978
authentication mac-move permit command 671
authentication priority command 672
available power 120

B

band-select command 979
boot command 812
broadcast-ssid command 980
budgeted power 120

C

cache command 42
cache-memory-max command 212
call-snoop command 981
cat command 813
ccx aironet-iesupport command 987
channel-group command 274
channel-protocol command 277
channel-scan defer-priority command 982
channel-scan defer-time command 983
chd command 984
Cisco Discovery Protocol (CDP) 956
Cisco Mobility Services Engine (MSE) 123
class command 590
class-map command 592
clear ap config 448
clear ap eventlog-all 448
clear ap join statistics 449
clear ap mac-address 449
clear ap name tsm dot11 all 447
clear ap name wlan statistics 450
clear errdisable interface vlan 676
clear ip mfib command 213
clear ip mroute command 214
clear lacp command 278
clear location command 814
clear location statistics command 815
clear mac address-table command 677
clear nmsp statistics command 816
clear pagp command 279
clear spanning-tree counters command 279
clear spanning-tree detected-protocols command 280
clear vtp counters command 939
clear wireless ccx statistics command 816
clear wireless client tsm dot11 command 817
clear wireless location s69 statistics command 818
clear wireless mobility statistics 523
client association limit command 985
client vlan command 101, 938, 986
collect command 46
collect counter command 47
collect interface command 48
collect timestamp absolute command 49
collect transport tcp flags command 50
consumed power 120

copy command 818

D

datalink flow monitor command 51, 988
debug ap mac-address 451
debug etherchannel command 281
debug flow exporter command 52
debug flow monitor command 53
debug ilpower command 102
debug interface command 103
debug lacp command 282
debug lldp packets command 104
debug nmsp command 105
debug pagp command 283
debug platform pm command 284
debug platform poe command 106
debug platform stack-manager command 762
debug platform udld command 286
debug platform vlan command 939
debug spanning-tree command 286
debug sw-vlan command 940
debug sw-vlan ifs command 941
debug sw-vlan notification command 942
debug sw-vlan vtp command 943
default ap dot11 rrm channel 27
default ap dot11 rrm channel cleanair-event 26
default ap dot11 rrm channel command 30
default command 990
delete command 824
deny command 678
description command 55
destination command 56
device-classification command 989
dir command 825
dot1x test timeout 687
dscp command 57
dtim dot11 command 992
duplex command 106

E

emergency-install command 826
epm access-control open command 690
errdisable detect cause command 108
errdisable recovery cause command 110
errdisable recovery interval command 112
exclusionlist command 993
exit command 828, 994
export-protocol netflow-v9 command 57

F

flash_init command 828
flow-based RSPAN (FRSPAN) session 546
flow-based SPAN (FSPAN) session 546
full-ring state 801

H

help command 829

I

interface command 113
interface port-channel command 288
interface range command 114
interface vlan command 945
ip access-group command 995
ip admission name command 692
ip device tracking maximum command 694
ip device tracking probe command 695
ip dhcp snooping verify no-relay-agent-address 698
ip flow monitor command 61, 996
ip igmp snooping last-member-query-count command 220
ip mtu command 115
ip multicast auto-enable command 226
ip multicast vlan command 226
ip verify source command 701
ip verify source mac-check command 997
ipv6 flow monitor command 62, 267
ipv6 mtu command 116
ipv6 traffic-filter command 268

L

lacp max-bundle command 289
lacp port-priority command 290
lacp system-priority command 292
license right-to-use 830
lldp (interface configuration) command 117
load-balance command 998
location algorithm command 835
location expiry command 835
location notify-threshold command 836
location plm calibrating command 837
location rfid command 838
location rssi-half-life command 839
logging event power-inline-status command 118

M

mab request format attribute 32 command 706
mac address-table move update command 840
main-cpu command 763
match (access-map configuration) command 707
match (class-map configuration) command 593
match datalink ethertype command 64
match datalink mac command 65
match datalink vlan command 66
match flow direction command 66
match interface command 67
match ipv4 command 68
match ipv4 destination address command 69
match ipv4 source address command 70
match ipv4 ttl command 71
match ipv6 command 71
match ipv6 destination address command 72
match ipv6 hop-limit command 73
match ipv6 source command 74
match non-client-nrt command 596
match transport command 74
match transport icmp ipv4 command 75
match transport icmp ipv6 command 76
match wlan user-priority command 597
maximum transmission unit (MTU) 192, 199
mdix auto command 119
media-stream multicast-direct command 932
mgmt_init command 841
mkdir command 842
mobility anchor 513, 999
mode (power-stack configuration) command 120
monitor session command 541, 542
monitor session filter command 546
monitor session source command 547
more command 842

N

nac command 1000
network-policy command 121
network-policy configuration mode 122
network-policy profile (global configuration) command 122
network-policy profiles 167
nmsp attachment suppress command 123
nmsp notification interval command 843
no authentication logging verbose 709
no dot1x logging verbose 709
no mab logging verbose 710

O

option command 78

P

pagp learn-method command 293
pagp port-priority command 294
partial-ring state 801
passive-client command 1001
peer-blocking command 1002
permit command 711
persistent MAC address 798
policy config-sync prc reload command 764
policy-map command 597
port-channel auto command 295
port-channel load-balance command 296
port-channel load-balance extended command 297
port-channel min-links command 299
power efficient-ethernet auto command 124
power inline command 126
power inline police command 129
power stack configuration mode 120
power supply command 131
power-priority command 124

Q

queue-limit command 603

R

radio command 1003
radio-policy command 1004
real-time power consumption policing 129
redistribute mdns-sd command 236
redundancy command 765
redundancy config-sync mismatched-commands command 766
redundancy force-switchover command 767
redundancy reload command 768
reload command 769
Remote SPAN (RSPAN) sessions 550
rename command 845
request platform software trace archive 924, 925
request platform software trace filter binary 925
reset command 846
rmdir command 847
roamed-voice-client re-anchor command 1005

RSPAN 541, 542, 546, 547
sessions 541, 542, 547
add interfaces to 541, 542, 547
start new 541, 542, 547

S

sdm prefer command 847
security passthru command 716
security web-auth command 1008
service-list mdns-sd service-list-name command 237
service-policy command 240, 604, 605, 1010
service-policy-query command 238
service-routing mdns-sd command 239
session command 770
session-timeout command 1011
set command 606, 848
set platform software trace 913, 917
set trace capwap ap ha command 771
set trace mobility ha command 772
set trace qos ap ha command 774
show ap cac voice 451
show ap capwap 452
show ap cdp 454
show ap config dot11 454
show ap config fnf 456
show ap config global 456
show ap crash-file 457
show ap data-plane 457
show ap dot11 459, 460
show ap dot11 24ghz cleanair device type command 648
show ap dot11 24ghz cleanair summary command 38
show ap dot11 24ghz command 930
show ap dot11 5ghz 461, 649
show ap dot11 5ghz cleanair device type command 34
show ap dot11 cleanair summary 461
show ap dot11 l2roam 458
show ap ethernet statistics 467
show ap groups 468
show ap image 469
show ap join stats summary 470
show ap link-encryption 471
show ap mac-address 471
show ap monitor-mode summary 473
show ap name 497
show ap name auto-rf 473
show ap name bhrate 476
show ap name cac voice 476
show ap name capwap retransmit 479
show ap name ccx rm 480
show ap name cdp neighbors 481
show ap name channel 481
show ap name command 475
show ap name config 482
show ap name config dot11 484
show ap name config fnf 477
show ap name config slot 487
show ap name core-dump 490
show ap name data-plane 491
show ap name dot11 491, 613
show ap name dot11 call-control 478
show ap name dot11 cleanair 494
show ap name ethernet statistics 495
show ap name eventlog 496
show ap name inventory 498
show ap name link-encryption 499
show ap name service-policy 500, 612
show ap name tcp-adjust-mss 501
show ap name wlan 501
show ap slots 503
show ap summary 504
show ap tcp-adjust-mss 504
show ap uptime 505
show avc client command 851
show avc wlan command 851
show cable-diagnostics tdr command 852
show capwap summary 132
show class-map command 615
show controller utilization command 143
show controllers cpu-interface command 133
show controllers ethernet-controller command 134
show eap command 725
show eee command 144
show env command 147, 856
show env xps command 857
show errdisable detect command 150
show errdisable recovery command 151
show etherchannel command 307
show flow exporter command 81
show flow record command 89
show interfaces command 152
show interfaces counters command 156
show interfaces switchport command 158
show interfaces transceiver command 160
show ip igmp snooping igmpv2-tracking command 245
show ip igmp snooping wireless mcast-spi-count command 248
show ip igmp snooping wireless mgid command 248
show ip pim autorp command 249
show ip pim bsr command 251
show ip pim bsr-router command 250
show ip pim tunnel command 252
show ip sla statistics command 549
show lacp command 310
show license right-to-use command 865
show location ap-detect command 868
show location command 867

show mac address-table move update command 869
show mgmt-infra trace messages ilpower command 165
show mgmt-infra trace messages ilpower-ha command 166
show mgmt-infra trace messages platform-mgr-poe command 166
show mod command 164
show monitor command 550
show network-policy profile command 167
show nmsp command 870
show pagp command 314
show platform capwap summary 168
show platform etherchannel command 315
show platform ip multicast command 256
show platform ip wccp command 553
show platform pm command 316
show platform software trace level 921
show platform software trace message 918
show platform stack-manager command 786
show platform vlan command 946
show policy-map command 626
show power inline command 185
show redundancy command 787
show redundancy config-sync command 790
show sampler command 89
show sdm prefer command 871
show stack-power command 190, 192
show storm-control 729
show switch command 792
show system mtu command 192
show tech-support command 193
show tech-support wireless command 872
show trace messages capwap ap ha command 796
show trace messages mobility ha command 797
show udld command 318
show vlan access-map command 731
show vlan command 946
show vlan filter command 732
show vlan group command 732
show vtp command 949
show wireless ap summary 506
show wireless band-select command 874
show wireless client ap 507
show wireless client calls command 622, 875
show wireless client dot11 command 623, 876
show wireless client location-calibration command 876
show wireless client mac-address command 624, 625
show wireless client probing command 877
show wireless client summary command 878
show wireless client timers command 878
show wireless client voice diagnostics command 625, 879
show wireless country command 880
show wireless detail command 883
show wireless dtls connections command 883
show wireless interface summary command 195
show wireless ipv6 statistics command 269
show wireless load-balancing command 886
show wireless media-stream group command 931
show wireless mobility 522
show wireless performance command 886
show wireless pmk-cache command 887
show wireless probe command 888
show wireless sip preferred-call-no command 888
show wireless summary command 889
show wireless vlan group command 955
show wlan command 628, 1012
shutdown command 890, 1015
sip-cac command 1016
snmp-server enable traps bridge command 558
snmp-server enable traps bulkstat command 559
snmp-server enable traps call-home command 560
snmp-server enable traps cef command 561
snmp-server enable traps command 556
snmp-server enable traps CPU command 562
snmp-server enable traps envmon command 563
snmp-server enable traps errdisable command 564
snmp-server enable traps flash command 565
snmp-server enable traps isis command 566
snmp-server enable traps license command 566
snmp-server enable traps mac-notification command 567
snmp-server enable traps ospf command 568
snmp-server enable traps pim command 569
snmp-server enable traps port-security command 570
snmp-server enable traps power-ethernet command 571
snmp-server enable traps snmp command 572
snmp-server enable traps stackwise command 573
snmp-server enable traps storm-control command 575
snmp-server enable traps stpx command 576
snmp-server enable traps transceiver command 577
snmp-server enable traps vrfmib command 578
snmp-server enable traps vstack command 579
snmp-server engineID command 580
snmp-server host command 580
speed command 195
stack member number 804
stack member priority 802
stack-mac persistent timer command 798
stack-mac update force command 799
stack-power command 197
StackPower 190, 192, 197
standby console enable command 800
static-ip tunneling command 1017
storm-control command 733
switch priority command 802
switch provision command 802
switch renumber command 804
switch stack port command 801
Switched Port Analyzer (SPAN) sessions 550
switchport access vlan command 323
switchport block command 198

switchport command 322
switchport mode access 585, 586
switchport mode command 324
switchport nonegotiate command 326
switchport port-security aging command 736
switchport port-security mac-address command 737
switchport port-security maximum command 739
switchport port-security violation command 741
switchport priority extend command 956
switchport trunk command 957
switchport voice vlan command 327
system env temperature threshold yellow command 891
system mtu command 199

T

template data timeout command 93
test ap name 508
test cable-diagnostics tdr command 892
test capwap ap name 508
test mcu read register command 200
traceroute mac command 893
traceroute mac ip command 895
transport command 93
trapflags ap 509
trapflags client command 898
trapflags command 897
ttl command 94
type command 899

U

udld command 329
udld port command 330
udld reset command 332
unset command 900

V

version command 901
vlan access-map command 754
vlan command 959, 1018
vlan dot1q tag native command 965
vlan filter command 756
vlan group command 757
voice vlan command 203
voice-signaling vlan command 202
vtp (global configuration) command 965
vtp (interface configuration) command 970
vtp primary command 971

W

wgb non-cisco command 1019
wireless ap-manager interface 204
wireless broadcast vlan command 972
wireless client command 902
wireless client mac-address command 904
wireless dot11-padding command 745
wireless exclusionlist command 205
wireless linktest command 206
wireless load-balancing command 909
wireless management interface command 207
wireless media-stream command 933
wireless mobility 515
wireless mobility controller 515, 517
wireless mobility group keepalive 518
wireless mobility group member ip 519
wireless mobility group name 520
wireless mobility load-balance 521
wireless multicast command 263
wireless peer-blocking forward-upstream command 207
wireless security dot1x command 745
wireless security lsc command 747
wireless security strong-password command 748
wireless sip preferred-call-no command 910
wireless wps ap-authentication command 749
wireless wps auto-immune command 750
wireless wps cids-sensor command 750
wireless wps client-exclusion command 751
wireless wps mfp infrastructure command 752
wireless wps rogue command 753
wireless wps shun-list re-sync command 754
wlan command 1021, 1022
wlan shutdown command 1023
wmm command 1023