



Consolidated Platform Command Reference, Cisco IOS XE 3.6E (Catalyst 3850 Switches)

First Published: 2014-06-27

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



CONTENTS

PREFACE

Preface xxix

Document Conventions xxix

Related Documentation xxxi

Obtaining Documentation and Submitting a Service Request xxxi

CHAPTER 1

Using the Command-Line Interface 1

Using the Command-Line Interface 2

Understanding Command Modes 2

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 6

Disabling the Command History Feature 6

Using Editing Features 6

Enabling and Disabling Editing Features 7

Editing Commands through Keystrokes 7

Editing Command Lines that Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI 10

Accessing the CLI through a Console Connection or through Telnet 11

PART I

CleanAir 13

CHAPTER 2

CleanAir Commands 15

ap dot11 5ghz cleanair 16

ap dot11 5ghz cleanair alarm air-quality 17

ap dot11 5ghz cleanair alarm device 18

default ap dot11 5ghz cleanair device 19

ap dot11 5ghz rrm channel cleanair-event 20

ap dot11 5ghz rrm channel device 21

ap dot11 24ghz cleanair 22

ap dot11 24ghz cleanair alarm air-quality 23

ap dot11 24ghz cleanair alarm device 24

default ap dot11 24ghz cleanair device 26

ap dot11 24ghz rrm channel cleanair-event 28

ap dot11 24ghz rrm channel device 29

ap name mode se-connect 30

default ap dot11 5ghz cleanair device 31

default ap dot11 5ghz rrm channel cleanair-event 32

default ap dot11 5ghz rrm channel device 33

default ap dot11 24ghz cleanair alarm device 34

default ap dot11 24ghz cleanair device 36

default ap dot11 24ghz rrm channel cleanair-event 38

show ap dot11 5ghz cleanair air-quality summary 39

show ap dot11 5ghz cleanair air-quality worst 40

show ap dot11 5ghz cleanair config 41

show ap dot11 5ghz cleanair device type 43

show ap dot11 24ghz cleanair air-quality summary 45

show ap dot11 24ghz cleanair air-quality worst 46

show ap dot11 24ghz cleanair config 47

show ap dot11 24ghz cleanair summary 49

PART II

Interface and Hardware Components 51

CHAPTER 3

Interface and Hardware Commands 53

client vlan 55

debug ilpower	56
debug interface	57
debug lldp packets	58
debug nmsp	59
debug platform poe	60
duplex	61
errdisable detect cause	63
errdisable recovery cause	65
errdisable recovery interval	68
interface	69
interface range	71
ip mtu	73
ipv6 mtu	75
lldp (interface configuration)	77
logging event power-inline-status	79
mdix auto	80
mode (power-stack configuration)	81
network-policy	83
network-policy profile (global configuration)	84
nmsp attachment suppress	85
power efficient-ethernet auto	86
power-priority	87
power inline	89
power inline police	93
power supply	95
show CAPWAP summary	97
show controllers cpu-interface	98
show controllers ethernet-controller	100
show controllers utilization	109
show eee	111
show env	114
show errdisable detect	117
show errdisable recovery	119
show interfaces	121

show interfaces counters 125

show interfaces switchport 127

show interfaces transceiver 131

show mgmt-infra trace messages ilpower 135

show mgmt-infra trace messages ilpower-ha 137

show mgmt-infra trace messages platform-mgr-poe 138

show network-policy profile 139

show platform CAPWAP summary 140

show power inline 141

show stack-power 147

show system mtu 148

show tech-support poe 149

show wireless interface summary 151

speed 152

stack-power 154

switchport backup interface 156

switchport block 158

system mtu 159

voice-signaling vlan (network-policy configuration) 160

voice vlan (network-policy configuration) 162

wireless ap-manager interface 164

wireless exclusionlist 165

wireless linktest 166

wireless management interface 167

wireless peer-blocking forward-upstream 168

PART III IPv6 169

CHAPTER 4 IPv6 Commands 171

ipv6 flow monitor 172

ipv6 traffic-filter 173

show wireless ipv6 statistics 174

PART IV Layer 2/3 175

CHAPTER 5**Layer 2/3 Commands 177**

channel-group	179
channel-protocol	182
clear lacp	183
clear pagp	184
clear spanning-tree counters	185
clear spanning-tree detected-protocols	186
debug etherchannel	187
debug lacp	188
debug pagp	189
debug platform pm	190
debug platform udd	192
debug spanning-tree	193
interface port-channel	195
lacp max-bundle	196
lacp port-priority	197
lacp system-priority	199
pagp learn-method	200
pagp port-priority	202
port-channel load-balance	203
port-channel load-balance extended	205
port-channel min-links	206
show etherchannel	207
show lacp	210
show pagp	214
show platform etherchannel	216
show platform pm	217
show udd	218
switchport	222
switchport access vlan	224
switchport mode	227
switchport nonegotiate	229
udd	230

udld port 232
 udld reset 234

PART V
Lightweight Access Point 235

CHAPTER 6
Cisco Lightweight Access Point Commands 237

ap auth-list ap-policy 242
 ap bridging 243
 ap capwap multicast 244
 ap capwap retransmit 245
 ap capwap timers 246
 ap cdp 248
 ap core-dump 249
 ap country 250
 ap crash-file 251
 ap dot11 24ghz preamble 252
 ap dot11 24ghz dot11g 253
 ap dot11 5ghz channelswitch mode 254
 ap dot11 5ghz power-constraint 255
 ap dot11 beaconperiod 256
 ap dot11 beamforming 257
 ap dot11 cac media-stream 258
 ap dot11 cac multimedia 261
 ap dot11 cac video 263
 ap dot11 cac voice 265
 ap dot11 cleanair 269
 ap dot11 cleanair alarm air-quality 270
 ap dot11 cleanair alarm device 271
 ap dot11 cleanair device 273
 ap dot11 dot11n 275
 ap dot11 dtpc 278
 ap dot11 edca-parameters 280
 ap dot11 rrm group-mode 281
 ap dot11 rrm channel cleanair-event 282

ap dot11 l2roam rf-params	283
ap dot11 media-stream	285
ap dot11 rrm ccx location-measurement	287
ap dot11 rrm channel dca	288
ap dot11 rrm group-member	290
ap dot11 rrm logging	291
ap dot11 rrm monitor	293
ap dot11 rrm ndp-type	295
ap dot11 5ghz dot11ac frame-burst	296
ap dot1x max-sessions	297
ap dot1x username	298
ap ethernet duplex	299
ap group	300
ap image	301
ap ipv6 tcp adjust-mss	302
ap led	303
ap link-encryption	304
ap link-latency	305
ap mgmtuser username	306
ap name ap-groupname	308
ap name antenna band mode	309
ap name bhrate	310
ap name bridgegroupname	311
ap name bridging	312
ap name cdp interface	313
ap name console-redirect	314
ap name capwap retransmit	315
ap name command	316
ap name core-dump	317
ap name country	318
ap name crash-file	319
ap name dot11 24ghz rrm coverage	320
ap name dot11 49ghz rrm profile	322
ap name dot11 5ghz rrm channel	324

ap name dot11 antenna	325
ap name dot11 antenna extantgain	327
ap name dot11 cleanair	328
ap name dot11 dot11n antenna	329
ap name dot11 dual-band cleanair	330
ap name dot11 dual-band shutdown	331
ap name dot11 rrm ccx	332
ap name dot11 rrm profile	333
ap name dot11 txpower	335
ap name dot1x-user	336
ap name ethernet	338
ap name ethernet duplex	339
ap name key-zeroize	340
ap name image	341
ap name ipv6 tcp adjust-mss	342
ap name jumbo mtu	343
ap name lan	344
ap name led	345
ap name link-encryption	346
ap name link-latency	347
ap name location	348
ap name mgmtuser	349
ap name mode	351
ap name monitor-mode	353
ap name monitor-mode dot11b	354
ap name name	355
ap name no dot11 shutdown	356
ap name power	357
ap name shutdown	358
ap name slot shutdown	359
ap name sniff	360
ap name ssh	361
ap name telnet	362
ap name power injector	363

ap name power pre-standard 364

ap name reset-button 365

ap name reset 366

ap name slot 367

ap name static-ip 369

ap name stats-timer 370

ap name syslog host 371

ap name syslog level 372

ap name tcp-adjust-mss 373

ap name tftp-downgrade 374

ap power injector 375

ap power pre-standard 376

ap reporting-period 377

ap reset-button 378

service-policy type control subscriber 379

ap static-ip 380

ap syslog 381

ap name no controller 382

ap tcp-adjust-mss size 383

ap tftp-downgrade 384

config wireless wps rogue client mse 385

clear ap name tsm dot11 all 386

clear ap config 387

clear ap eventlog-all 388

clear ap join statistics 389

clear ap mac-address 390

clear ap name wlan statistics 391

debug ap mac-address 392

show ap cac voice 393

show ap capwap 395

show ap cdp 397

show ap config dot11 398

show ap config dot11 dual-band summary 399

show ap config fnf 400

show ap config	401
show ap crash-file	402
show ap data-plane	403
show ap dot11 l2roam	404
show ap dot11 cleanair air-quality	405
show ap dot11 cleanair config	406
show ap dot11 cleanair summary	408
show ap dot11	409
show ap env summary	415
show ap ethernet statistics	416
show ap gps-location summary	417
show ap groups	418
show ap groups extended	419
show ap image	420
show ap is-supported	421
show ap join stats summary	422
show ap link-encryption	423
show ap mac-address	424
show ap monitor-mode summary	426
show ap name auto-rf	427
show ap name bhmode	430
show ap name bhrate	431
show ap name cac voice	432
show ap name config fnf	433
show ap name dot11 call-control	434
show ap name cable-modem	435
show ap name capwap retransmit	436
show ap name ccx rm	437
show ap name cdp	438
show ap name channel	439
show ap name config	440
show ap name config dot11	442
show ap name config slot	446
show ap name core-dump	450

show ap name data-plane	451
show ap name dot11	452
show ap name dot11 cleanair	455
show ap name env	456
show ap name ethernet statistics	457
show ap name eventlog	458
show ap gps-location summary	459
show ap name image	460
show ap name inventory	461
show ap name lan port	462
show ap name link-encryption	463
show ap name service-policy	464
show ap name tcp-adjust-mss	465
show ap name wlan	466
show ap name wlandot11 service policy	468
show ap slots	469
show ap summary	470
show ap tcp-adjust-mss	471
show ap universal summary	472
show ap uptime	473
show wireless ap summary	474
show wireless client ap	475
test ap name	476
test capwap ap name	477
trapflags ap	478
wireless probe filter	479
wireless probe limit	480
wireless wps rogue ap rldp alarm-only	481
wireless wps rogue ap rldp auto-contain	482

PART VI**Mobility 483**

CHAPTER 7**Mobility Commands 485**

mobility anchor 486

wireless mobility	488
wireless mobility controller	489
wireless mobility controller (ip_address)	491
wireless mobility controller peer-group	492
wireless mobility group keepalive	493
wireless mobility group member ip	494
wireless mobility group name	495
wireless mobility load-balance	496
show wireless mobility	497
clear wireless mobility statistics	498

PART VII
Network Management 499

CHAPTER 8
Network Management 501

ip wccp	503
monitor capture (interface/control plane)	505
monitor capture buffer	509
monitor capture clear	510
monitor capture export	511
monitor capture file	512
monitor capture limit	514
monitor capture match	515
monitor capture start	516
monitor capture stop	517
monitor session	518
monitor session destination	520
monitor session filter	524
monitor session source	526
show ip sla statistics	529
show monitor	531
show monitor capture	534
show platform ip wccp	536
snmp-server enable traps	537
snmp-server enable traps bridge	540

snmp-server enable traps bulkstat	541
snmp-server enable traps call-home	542
snmp-server enable traps cef	543
snmp-server enable traps cpu	544
snmp-server enable traps envmon	545
snmp-server enable traps errdisable	546
snmp-server enable traps flash	547
snmp-server enable traps isis	548
snmp-server enable traps license	549
snmp-server enable traps mac-notification	550
snmp-server enable traps ospf	551
snmp-server enable traps pim	552
snmp-server enable traps port-security	553
snmp-server enable traps power-ethernet	554
snmp-server enable traps snmp	555
snmp-server enable traps stackwise	556
snmp-server enable traps storm-control	558
snmp-server enable traps stpx	559
snmp-server enable traps transceiver	560
snmp-server enable traps vrfmib	561
snmp-server enable traps vstack	562
snmp-server engineID	563
snmp-server host	564
switchport mode access	568
switchport voice vlan	569

PART VIII
QoS 571

CHAPTER 9
QoS 573

auto qos	574
class	575
class-map	578
match (class-map configuration)	580
match non-client-nrt	583

- match wlan user-priority 584
- policy-map 585
- priority 588
- qos queue-softmax-multiplier 590
- queue-buffers ratio 591
- queue-limit 592
- service-policy (Wired) 594
- service-policy (WLAN) 596
- set 597
- show ap name service-policy 604
- show ap name dot11 605
- show class-map 608
- show wireless client calls 609
- show wireless client dot11 610
- show wireless client mac-address (Call Control) 611
- show wireless client mac-address (TCLAS) 612
- show wireless client voice diagnostics 613
- show policy-map 614
- show wlan 619
- trust device 622

CHAPTER 10

Auto-QoS 625

- auto qos classify 626
- auto qos trust 632
- auto qos video 640
- auto qos voip 651
- debug auto qos 664
- show auto qos 665

PART IX

Radio Resource Management 667

CHAPTER 11

Radio Resource Management Commands 669

- airtime-fairness dot11 mode (apgroup) 671
- airtime-fairness dot11 optimization (apgroup) 672

airtime-fairness dot11 policy	673
airtime-fairness policy (wlan)	674
ap dot11 rf-profile	675
ap dot11 rrm	676
ap dot11 rrm ccx	679
ap dot11 rrm channel	680
ap dot11 24ghz rrm channel cleanair-event rogue-contribution	681
ap dot11 24ghz or 5ghz rrm channel dca add	682
ap dot11 24ghz or 5ghz rrm channel dca remove	683
ap dot11 5ghz rrm channel dca chan-width width-max	684
ap dot11 rrm coverage	685
ap dot11 rrm group-member	687
ap dot11 rrm monitor	688
ap dot11 rrm profile	689
ap dot11 rrm tpc-threshold	690
ap dot11 rrm txpower	691
ap dot11 airtime-fairness mode	692
ap dot11 airtime-fairness policy-name	693
policy-weight	693
ap group	695
ap name dot11 airtime-fairness mode	696
ap name dot11 airtime-fairness optimization	697
ap name no dot11 airtime-fairness wlan-name policy-name	698
ap name dot11 airtime-fairness wlan-name policy	699
band-select client	700
band-select cycle	701
band-select expire	702
band-select probe-response	703
channel	704
channel foreign	705
channel width	706
coverage	707
coverage exception	708
coverage level	709

clear wireless airtime-fairness statistics	710
dot11n-only	711
load-balancing	712
high-density clients count	713
high-density clients wlan	714
high-density multicast data-rate	715
high-density rx-sop threshold	716
rate	717
rate mcs	718
trap threshold	719
tx-power	720
tx-power vl threshold	721
no ap dot11 airtime-fairness policy-name	722
remote-lan	723
rf-profile dot11 24ghz	724
rf-profile dot11 5ghz	725
show ap airtime-fairness ap-group	726
show ap airtime-fairness (ap)	727
show ap airtime-fairness (per radio)	728
show ap airtime-fairness policy (all)	729
show ap airtime-fairness wlan	730
show ap dot11 24ghz	731
show ap dot11 5ghz	733
show ap dot11 airtime-fairness (radio bands)	735
show ap dot11 24ghz rf-profile summary	736
show ap dot11 5ghz rf-profile summary	737
show ap name dot11 airtime-fairness summary	738
show ap name dot11 airtime-fairness policy statistics	739
show ap name dot11 airtime-fairness wlan name statistics	740
show ap rf-profile summary	741
show ap rf-profile name	742
show wireless mobility controller ap	744
shutdown	745
wlan	746

PART X**Security 747**

CHAPTER 12**Security 749**

- aaa accounting dot1x 752
- aaa accounting identity 754
- aaa authentication dot1x 756
- aaa authorization 757
- aaa new-model 761
- access-session mac-move deny 763
- action 765
- authentication host-mode 766
- authentication mac-move permit 768
- authentication priority 770
- authentication violation 773
- auto security 775
- auto security-port 776
- cisp enable 777
- clear errdisable interface vlan 778
- clear mac address-table 779
- debug ip rip 781
- deny (MAC access-list configuration) 783
- device-role (IPv6 snooping) 787
- device-role (IPv6 nd inspection) 788
- device-tracking policy 789
- dot1x critical (global configuration) 791
- dot1x max-start 792
- dot1x pae 793
- dot1x supplicant force-multicast 794
- dot1x test eapol-capable 795
- dot1x test timeout 796
- dot1x timeout 797
- epm access-control open 799
- ip admission 800

ip admission name	801
ip device tracking maximum	803
ip device tracking probe	804
ip dhcp snooping database	805
ip dhcp snooping information option format remote-id	807
ip dhcp snooping verify no-relay-agent-address	808
ip source binding	809
ip verify source	810
ipv6 snooping policy	812
limit address-count	813
mab request format attribute 32	814
match (access-map configuration)	816
authentication logging verbose	818
dot1x logging verbose	819
mab logging verbose	820
permit (MAC access-list configuration)	821
protocol (IPv6 snooping)	825
radius server	826
router rip	828
security level (IPv6 snooping)	829
security passthru	830
show aaa clients	831
show aaa command handler	832
show aaa local	833
show aaa servers	834
show aaa sessions	835
show authentication history	836
show authentication sessions	837
show auto security	840
show cisp	842
show dot1x	844
show eap pac peer	846
show ip dhcp snooping statistics	847
show ip rip database	850

show radius server-group	852
show storm-control	854
show vlan access-map	856
show vlan filter	857
show vlan group	858
storm-control	859
switchport port-security aging	862
switchport port-security mac-address	864
switchport port-security maximum	867
switchport port-security violation	869
tracking (IPv6 snooping)	871
trusted-port	873
wireless dot11-padding	874
wireless security dot1x	875
wireless security lsc	877
wireless security strong-password	878
wireless wps ap-authentication	879
wireless wps auto-immune	880
wireless wps cids-sensor	881
wireless wps client-exclusion	882
wireless wps mfp infrastructure	884
wireless wps rogue	885
wireless wps shun-list re-sync	886
vlan access-map	887
vlan filter	889
vlan group	890

PART XI**Stack Manager and High Availability 891**

CHAPTER 13**Stack Manager and High Availability 893**

debug platform stack-manager	894
main-cpu	895
mode sso	896
policy config-sync prc reload	897

redundancy	898
redundancy config-sync mismatched-commands	899
redundancy force-switchover	901
redundancy reload	902
reload	903
session	905
set trace capwap ap ha	906
set trace mobility ha	907
set trace qos ap ha	909
show checkpoint	910
show etherchannel summary	917
show platform ses	918
show platform stack-manager	924
show redundancy	925
show redundancy config-sync	929
show switch	931
show trace messages capwap ap ha	935
show trace messages mobility ha	936
stack-mac persistent timer	937
stack-mac update force	939
standby console enable	940
switch stack port	941
switch priority	943
switch provision	944
switch renumber	946

PART XII
System Management 947

CHAPTER 14
System Management Commands 949

arp	952
boot	953
cat	954
clear location	955
clear location statistics	956

clear nmsp statistics 957
clear wireless ccx statistics 958
clear wireless client tsm dot11 959
clear wireless location s69 statistics 960
copy 961
copy startup-config tftp: 962
copy tftp: startup-config 963
debug call-admission wireless all 964
debug rfid 965
debug voice diagnostics mac-address 966
debug wps mfp 967
delete 968
dir 969
emergency-install 971
exit 973
flash_init 974
help 975
license right-to-use 976
location 978
location algorithm 982
location expiry 983
location notify-threshold 984
location plm calibrating 985
location rfid 986
location rssi-half-life 987
mac address-table move update 988
mgmt_init 989
mkdir 990
more 991
nmsp notification interval 992
no debug all 994
rename 995
reset 996
rmdir 997

sdm prefer	998
set	999
show ap name config general	1002
show avc client	1004
show avc wlan	1005
show cable-diagnostics tdr	1006
show debug	1008
show env	1009
show flow monitor	1012
show license right-to-use	1017
show location	1019
show location ap-detect	1020
show mac address-table move update	1022
show nmsp	1023
show sdm prefer	1024
show tech-support wireless	1026
show wireless ap summary (MA)	1028
show wireless ap summary	1029
show wireless band-select	1030
show wireless client calls	1031
show wireless client dot11	1032
show wireless client location-calibration	1033
show wireless client probing	1034
show wireless client summary	1035
show wireless client timers	1036
show wireless client voice diagnostics	1037
show wireless country	1038
show wireless detail	1041
show wireless dtls connections	1042
show wireless flow-control	1043
show wireless flow-control statistics	1044
show wireless load-balancing	1045
show wireless mobility summary	1046
show wireless performance	1047

[show wireless pmk-cache](#) 1048
[show wireless probe](#) 1049
[show wireless sip preferred-call-no](#) 1050
[show wireless summary](#) 1051
[show wireless wlan summary](#) 1052
[show wlan name](#) 1053
[shutdown](#) 1056
[system env temperature threshold yellow](#) 1057
[test cable-diagnostics tdr](#) 1059
[traceroute mac](#) 1060
[traceroute mac ip](#) 1063
[trapflags](#) 1065
[trapflags client](#) 1066
[type](#) 1067
[unset](#) 1068
[version](#) 1070
[wireless client](#) 1071
[wireless client mac-address deauthenticate](#) 1073
[wireless client mac-address](#) 1074
[wireless load-balancing](#) 1079
[wireless sip preferred-call-no](#) 1080

PART XIII
VideoStream 1081

CHAPTER 15
VideoStream Commands 1083

[ap dot11 media-stream multicast-direct](#) 1084
[show ap dot11](#) 1085
[show wireless media-stream group](#) 1086
[wireless media-stream multicast-direct](#) 1087
[wireless media-stream](#) 1088

PART XIV
VLAN 1091

CHAPTER 16
VLAN 1093

client vlan	1094
clear vtp counters	1095
debug platform vlan	1096
debug sw-vlan	1097
debug sw-vlan ifs	1099
debug sw-vlan notification	1100
debug sw-vlan vtp	1102
interface vlan	1104
show platform vlan	1106
show vlan	1107
show vtp	1110
show wireless vlan group	1116
switchport priority extend	1117
switchport trunk	1118
vlan	1121
vlan dot1q tag native	1127
vtp (global configuration)	1128
vtp (interface configuration)	1133
vtp primary	1134
wireless broadcast vlan	1135

PART XV**WLAN 1137**

CHAPTER 17**WLAN Commands 1139**

aaa-override	1141
accounting-list	1142
assisted-roaming	1143
ap name ap-name lan port-id port-id poe	1144
ap name ap-name lan override	1145
band-select	1146
broadcast-ssid	1147
call-snoop	1148
channel-scan defer-priority	1149
channel-scan defer-time	1150

chd	1151
client association limit	1152
client vlan	1154
ccx aironet-iesupport	1155
datalink flow monitor	1156
device-classification	1157
default	1158
dtim dot11	1161
exclusionlist	1162
exit	1163
exit (WLAN AP Group)	1164
ip access-group	1165
ip flow monitor	1166
ip verify source mac-check	1167
load-balance	1168
mobility anchor	1169
nac	1171
passive-client	1172
peer-blocking	1173
port	1174
poe	1175
radio	1176
radio-policy	1177
remote-lan	1178
remote-lan	1179
roamed-voice-client re-anchor	1180
security ft	1181
security pmf	1183
security web-auth	1185
security wpa akm	1186
service-policy (WLAN)	1188
session-timeout	1189
show remote-lan all	1190
show remote-lan id	1191

show remote-lan name	1192
show remote-lan summary	1193
show running-config remote-lan	1194
show wlan	1195
show wireless wlan summary	1198
shutdown	1199
sip-cac	1200
static-ip tunneling	1201
vlan	1202
universal-admin	1203
wgb non-cisco	1204
wifidirect policy	1205
wlan (AP Group Configuration)	1206
wlan	1207
wlan shutdown	1208
wmm	1209



Preface

- [Document Conventions](#) , on page xxix
- [Related Documentation](#), on page xxxi
- [Obtaining Documentation and Submitting a Service Request](#), on page xxxi

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 .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
Courier font	Terminal sessions and information the system displays appear in <code>courier font</code> .
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.
{x y}	Required alternative keywords are grouped in braces and separated by vertical bars.

Convention	Description
[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 switch, refer to the switch release notes.

- Cisco Catalyst 3850 Series Switches 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>

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.



Using the Command-Line Interface

This chapter contains the following topics:

- [Using the Command-Line Interface, on page 2](#)

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 <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Switch#	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.	Switch(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.

Mode	Access Method	Prompt	Exit Method	About This Mode
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Switch(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).	Switch(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.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Switch(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.
<i>abbreviated-command-entry ?</i> Switch# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.

Command	Purpose
<p><i>abbreviated-command-entry</i> <Tab></p> <pre>Switch# sh conf<tab> Switch# show configuration</pre>	Completes a partial command name.
<p>?</p> <pre>Switch> ?</pre>	Lists all commands available for a particular command mode.
<p><i>command ?</i></p> <pre>Switch> show ?</pre>	Lists the associated keywords for a command.
<p><i>command keyword ?</i></p> <pre>Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet</pre>	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:

```
Switch# 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:

```
Switch# 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:

```
Switch(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 Switch(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:

```
Switch# terminal editing
```

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

```
Switch(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.

Capability	Keystroke	Purpose
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.
	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 .	

Capability	Keystroke	Purpose
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.

```
Switch(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1
Switch(config)# $ 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.25
Switch(config)# $t tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq
Switch(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:

```
Switch(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:

```
Switch# 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, on page 15](#)



CleanAir Commands

- [ap dot11 5ghz cleanair](#) , on page 16
- [ap dot11 5ghz cleanair alarm air-quality](#), on page 17
- [ap dot11 5ghz cleanair alarm device](#), on page 18
- [default ap dot11 5ghz cleanair device](#), on page 19
- [ap dot11 5ghz rrm channel cleanair-event](#), on page 20
- [ap dot11 5ghz rrm channel device](#), on page 21
- [ap dot11 24ghz cleanair](#), on page 22
- [ap dot11 24ghz cleanair alarm air-quality](#), on page 23
- [ap dot11 24ghz cleanair alarm device](#), on page 24
- [default ap dot11 24ghz cleanair device](#), on page 26
- [ap dot11 24ghz rrm channel cleanair-event](#), on page 28
- [ap dot11 24ghz rrm channel device](#), on page 29
- [ap name mode se-connect](#), on page 30
- [default ap dot11 5ghz cleanair device](#), on page 31
- [default ap dot11 5ghz rrm channel cleanair-event](#), on page 32
- [default ap dot11 5ghz rrm channel device](#), on page 33
- [default ap dot11 24ghz cleanair alarm device](#), on page 34
- [default ap dot11 24ghz cleanair device](#), on page 36
- [default ap dot11 24ghz rrm channel cleanair-event](#), on page 38
- [show ap dot11 5ghz cleanair air-quality summary](#), on page 39
- [show ap dot11 5ghz cleanair air-quality worst](#), on page 40
- [show ap dot11 5ghz cleanair config](#), on page 41
- [show ap dot11 5ghz cleanair device type](#), on page 43
- [show ap dot11 24ghz cleanair air-quality summary](#), on page 45
- [show ap dot11 24ghz cleanair air-quality worst](#), on page 46
- [show ap dot11 24ghz cleanair config](#), on page 47
- [show ap dot11 24ghz cleanair summary](#), on page 49

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:

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

Related Topics

- [ap dot11 5ghz cleanair alarm air-quality](#), on page 17
- [ap dot11 5ghz cleanair alarm device](#), on page 18
- [default ap dot11 5ghz cleanair device](#), on page 19
- [ap dot11 5ghz rrm channel cleanair-event](#), on page 20
- [ap dot11 5ghz rrm channel device](#), on page 21

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 <i>threshold_value</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>You must enable CleanAir using the ap dot11 5ghz cleanair command before you configure this command.</p> <p>This example shows how to set the threshold value for the AQ:</p> <pre>Switch(config)# ap dot11 5ghz cleanair alarm air-quality threshold 30</pre>				

Related Topics

[ap dot11 5ghz cleanair](#), on page 16

[default ap dot11 5ghz cleanair device](#), on page 19

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:

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

Related Topics

[ap dot11 5ghz cleanair](#) , on page 16

[ap dot11 5ghz cleanair alarm air-quality](#), on page 17

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:

```
Switch(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:

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

Related Topics

[ap dot11 5ghz cleanair](#) , on page 16

[ap dot11 5ghz rrm channel device](#), on page 21

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 switch. 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:

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

Related Topics

[ap dot11 5ghz cleanair](#), on page 16

[ap dot11 5ghz rrm channel cleanair-event](#), on page 20

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:

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

Related Topics

- [ap dot11 24ghz cleanair alarm air-quality](#), on page 23
- [ap dot11 24ghz cleanair alarm device](#), on page 24
- [default ap dot11 24ghz cleanair device](#), on page 26
- [ap dot11 24ghz rrm channel cleanair-event](#), on page 28
- [ap dot11 24ghz rrm channel device](#), on page 29

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 <i>threshold_value</i> 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:

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

Related Topics

- [ap dot11 24ghz cleanair](#), on page 22
- [ap dot11 24ghz cleanair alarm device](#), on page 24
- [default ap dot11 24ghz cleanair device](#), on page 26

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:

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

Related Topics

[ap dot11 24ghz cleanair](#), on page 22

[ap dot11 24ghz cleanair alarm air-quality](#), on page 23

[default ap dot11 24ghz cleanair device](#), on page 26

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 {ble-beacon|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		
	ble-beacon	Configure the BLE beacon feature.
	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.
Cisco IOS XE Denali 16.2.1	This command was modified. The ble-beacon keyword was added.

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:

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

Related Topics

- [ap dot11 24ghz cleanair](#), on page 22
- [ap dot11 24ghz cleanair alarm air-quality](#), on page 23
- [ap dot11 24ghz cleanair alarm device](#), on page 24

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:

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

Related Topics

- [ap dot11 24ghz cleanair](#), on page 22
- [ap dot11 24ghz rrm channel device](#), on page 29

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 switch. Local and bridge mode access points detect interference devices on the serving channels only.

This example shows how to enable persistent device avoidance:

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

Related Topics

[ap dot11 24ghz cleanair](#), on page 22

[ap dot11 24ghz rrm channel cleanair-event](#), on page 28

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	<i>ap_name</i>	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:

```
Switch# 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	Parameter	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:

```
Switch(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:

```
Switch(config)# default ap dot11 5ghz rrm channel cleanair-event
Switch(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:

```
Switch(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:

```
Switch(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 {ble-beacon|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		
	ble-beacon	Configure the BLE beacon feature.
	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.
Cisco IOS XE Denali 16.2.1	This command was modified. The ble-beacon keyword was added.

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:

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

Related Topics

- [ap dot11 24ghz cleanair](#), on page 22
- [ap dot11 24ghz cleanair alarm air-quality](#), on page 23
- [ap dot11 24ghz cleanair alarm device](#), on page 24

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:

```
Switch(config)# default ap dot11 24ghz rrm channel cleanair-event
Switch(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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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.
	wimax-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:

```
Switch# 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
```

```
show ap dot11 5ghz cleanair device type
```

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

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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

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

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



PART II

Interface and Hardware Components

- [Interface and Hardware Commands, on page 53](#)



Interface and Hardware Commands

- [client vlan](#), on page 55
- [debug ilpower](#), on page 56
- [debug interface](#), on page 57
- [debug lldp packets](#), on page 58
- [debug nmsp](#), on page 59
- [debug platform poe](#), on page 60
- [duplex](#), on page 61
- [errdisable detect cause](#), on page 63
- [errdisable recovery cause](#), on page 65
- [errdisable recovery interval](#), on page 68
- [interface](#), on page 69
- [interface range](#), on page 71
- [ip mtu](#), on page 73
- [ipv6 mtu](#), on page 75
- [lldp \(interface configuration\)](#), on page 77
- [logging event power-inline-status](#), on page 79
- [mdix auto](#), on page 80
- [mode \(power-stack configuration\)](#), on page 81
- [network-policy](#), on page 83
- [network-policy profile \(global configuration\)](#), on page 84
- [nmsp attachment suppress](#), on page 85
- [power efficient-ethernet auto](#), on page 86
- [power-priority](#) , on page 87
- [power inline](#), on page 89
- [power inline police](#), on page 93
- [power supply](#), on page 95
- [show CAPWAP summary](#), on page 97
- [show controllers cpu-interface](#), on page 98
- [show controllers ethernet-controller](#), on page 100
- [show controllers utilization](#), on page 109
- [show eee](#), on page 111
- [show env](#), on page 114
- [show errdisable detect](#), on page 117

- [show errdisable recovery](#), on page 119
- [show interfaces](#), on page 121
- [show interfaces counters](#), on page 125
- [show interfaces switchport](#), on page 127
- [show interfaces transceiver](#), on page 131
- [show mgmt-infra trace messages ilpower](#), on page 135
- [show mgmt-infra trace messages ilpower-ha](#), on page 137
- [show mgmt-infra trace messages platform-mgr-poe](#), on page 138
- [show network-policy profile](#), on page 139
- [show platform CAPWAP summary](#), on page 140
- [show power inline](#), on page 141
- [show stack-power](#) , on page 147
- [show system mtu](#), on page 148
- [show tech-support poe](#), on page 149
- [show wireless interface summary](#), on page 151
- [speed](#), on page 152
- [stack-power](#) , on page 154
- [switchport backup interface](#), on page 156
- [switchport block](#), on page 158
- [system mtu](#), on page 159
- [voice-signaling vlan \(network-policy configuration\)](#), on page 160
- [voice vlan \(network-policy configuration\)](#), on page 162
- [wireless ap-manager interface](#), on page 164
- [wireless exclusionlist](#), on page 165
- [wireless linktest](#), on page 166
- [wireless management interface](#), on page 167
- [wireless peer-blocking forward-upstream](#), on page 168

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	<i>interface-id-name-or-group-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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		
	<i>interface-id</i>	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 <i>switch-number</i>	(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 <i>switch-number</i>	(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 reenables the interface during the reconfiguration.

You can verify your setting by entering the **show interfaces** privileged EXEC command.

Examples

This example shows how to configure an interface for full-duplex operation:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# duplex full
```

Related Topics

[show interfaces](#), on page 121

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:

```
Switch(config)# errdisable detect cause link-flap
```

This command shows how to globally configure BPDU guard for a per-VLAN error-disabled state:

```
Switch(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:

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

Related Topics

[show errdisable detect](#), on page 117

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

```
{[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}
```

no errdisable recovery cause

```
{[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}
```

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.
vmmps	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 BDPU 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.

Examples

This example shows how to enable the recovery timer for the BDPU guard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

Related Topics

[errdisable recovery interval](#), on page 68

[show errdisable recovery](#), on page 119

[show interfaces](#), on page 121

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	<i>timer-interval</i> 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.

Examples

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

Related Topics

- [errdisable recovery cause](#), on page 65
- [show errdisable recovery](#), on page 119
- [show interfaces](#), on page 121

interface

To configure an interface, use the **interface** command.

interface {**Auto-Template** *interface-number* | **Capwap** *Capwap interface-number* | **GigabitEthernet** *switch-number/slot-number/port-number* | **Group VI** *Group VI interface number* | **Internal Interface** *Internal Interface number* | **Loopback** *interface-number* | **Null** *interface-number* | **Port-channel** *interface-number* | **TenGigabitEthernet** *switch-number/slot-number/port-number* | **Tunnel** *interface-number* | **Vlan** *interface-number* }

Auto-Template <i>interface-number</i>	Enables you to configure a auto-template interface. The range is from 1 to 999.
Capwap <i>Capwap interface number</i>	Enables you to configure a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel interface. The range is from 0 to 2147483647.
GigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a Gigabit Ethernet IEEE 802.3z interface. The range is from 0 to 9
Group VI <i>Group VI interface number</i>	Enables you to configure a Group VI interface. The range is from 0 to 9.
Internal Interface <i>Internal Interface</i>	Enables you to configure an internal interface.
Loopback <i>interface-number</i>	Enables you to configure a loopback interface. The range is from 0 to 2147483647.
Null <i>interface-number</i>	Enables you to configure a null interface. The default value is 0.
Port-channel <i>interface-number</i>	Enables you to configure a port-channel interface. The range is from 1 to 128.
TenGigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a 10-Gigabit Ethernet interface. <ul style="list-style-type: none"> • <i>switch-number</i> — Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. The range is from 0 to 1. • <i>port-number</i> — Port number. The range is from 1 to 24 and 37 to 48
Tunnel <i>interface-number</i>	Enables you to configure a tunnel interface. The range is from 0 to 2147483647.
Vlan <i>interface-number</i>	Enables you to configure a switch VLAN. The range is from 1 to 4094.

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.

The following example shows how to configure a tunnel interface:

```
Switch# interface Tunnel 15
```

interface range

To configure an interface range, use the **interface range** command.

interface range { **GigabitEthernet** *switch-number/slot-number/port-number* | **Loopback** *interface-number* | **Port-channel** *interface-number* | **TenGigabitEthernet** *switch-number/slot-number/port-number* | **Tunnel** *interface-number* | **Vlan** *interface-number* | **MacroWORD** }

GigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a Gigabit Ethernet IEEE 802.3z interface. <ul style="list-style-type: none"> • <i>switch-number</i>— Switch ID. The range is from 1 to 8. • <i>slot-number</i> — Slot number. The range is from 0 to 1. • <i>port-number</i> — Port number. The range is from 1 to 48.
Loopback <i>interface-number</i>	Enables you to configure a loopback interface. The range is from 0 to 2147483647.
Port-channel <i>interface-number</i>	Enables you to configure a port-channel interface. The range is from 1 to 128.
TenGigabitEthernet <i>switch-number/slot-number/port-number</i>	Enables you to configure a 10-Gigabit Ethernet interface. <ul style="list-style-type: none"> • <i>switch-number</i>— Switch ID. The range is from 1 to 8. • <i>slot-number</i>— Slot number. The range is from 0 to 1. • <i>port-number</i>— Port number. The range is from 1 to 24 and 37 to 48.
Tunnel <i>interface-number</i>	Enables you to configure a tunnel interface. The range is from 0 to 2147483647.
Vlan <i>interface-number</i>	Enables you to configure a switch VLAN. The range is from 1 to 4094.
Macro <i>WORD</i>	Enables you to configure 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:

```
Switch(config)# interface range vlan 1-100
```

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	<i>bytes</i> 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:

```
Switch(config)# interface vlan 200
Switch(config-if)# ip mtu 1000
```

The following example sets the maximum IP packet size for VLAN 200 to the default setting of 1500 bytes:

```
Switch(config)# interface vlan 200
Switch(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.

```
Switch# 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>
```

Related Topics

[show interfaces](#), on page 121

[system mtu](#), on page 159

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	<i>bytes</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch(config)# interface gigabitethernet4/0/1
Switch(config-if)# ipv6 mtu 2000
```

The following example sets the maximum IPv6 packet size for an interface to the default setting of 1500 bytes:

```
Switch(config)# interface gigabitethernet4/0/1
Switch(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.

```
Switch# 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>
```

Related Topics

[show interfaces](#), on page 121

[system mtu](#), on page 159

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.
<i>tlv</i>		String that identifies the TLV element. Valid values are the following: <ul style="list-style-type: none"> • 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 disabled.

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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no lldp transmit
```

The following example shows how to enable LLDP transmission on an interface:

```
Switch(config)# interface gigabitethernet1/0/1
```

```
Switch(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.

Examples

This example shows how to enable logging of PoE events on a port:

```
Switch(config-if)# interface gigabitethernet1/0/1
Switch(config-if)# logging event power-inline-status
Switch(config-if)#
```

Related Topics

[power inline](#), on page 89

[show power inline](#), on page 141

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:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

Related Topics

[show controllers ethernet-controller](#), on page 100

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	redundant	strict
	Sets the power stack to operate in power-shared mode. This is the default.	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.	(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.

```
Switch(config)# stack-power stack power1  
Switch(config-stackpower)# mode power-shared strict  
Switch(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.

```
Switch(config)# stack-power stack power2  
Switch(config-stackpower)# mode redundant  
Switch(config-stackpower)# exit
```

Related Topics

[stack-power](#), on page 154

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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# network-policy 60
```

Related Topics

- [network-policy profile \(global configuration\)](#), on page 84
- [show network-policy profile](#), on page 139
- [voice-signaling vlan \(network-policy configuration\)](#), on page 160
- [voice vlan \(network-policy configuration\)](#), on page 162

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	<i>profile-number</i> 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:

```
Switch(config)# network-policy profile 60
Switch(config-network-policy)#
```

Related Topics

- [network-policy](#), on page 83
- [show network-policy profile](#), on page 139
- [voice-signaling vlan \(network-policy configuration\)](#), on page 160
- [voice vlan \(network-policy configuration\)](#), on page 162

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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# nmsp attachment suppress
```

Related Topics

[show nmsp](#)

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	<p>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.</p>
-------------------------	--

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 switch 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:

```
Switch(config-if)# power efficient-ethernet auto
Switch(config-if)#
```

This example shows how to disable EEE for an interface:

```
Switch(config-if)# no power efficient-ethernet auto
Switch(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 <i>value</i>	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 <i>value</i>	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 <i>value</i>	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.

Examples

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.

```
Switch(config)# stack-power switch 1  
Switch(config-switch-stackpower)# stack-id power_stack_a  
Switch(config-switch-stackpower)# power-priority high 11  
Switch(config-switch-stackpower)# power-priority low 20  
Switch(config-switch-stackpower)# power-priority switch 7  
Switch(config-switch-stackpower)# exit
```

Related Topics

[stack-power](#) , on page 154

[show stack-power](#) , on page 147

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 <i>max-wattage</i>		(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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(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 802.3at 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.

Examples

This example shows how to enable detection of a powered device and to automatically power a PoE port on a switch:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
```

```
Switch(config-if)# power inline port priority high
```

Related Topics

[logging event power-inline-status](#), on page 79

[show power inline](#), on page 141

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 switch 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 switch 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 switch 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 switch takes action when a powered device consumes more power than the allocated maximum amount.

When PoE is enabled, the switch senses the real-time power consumption of the powered device. This feature is called *power monitoring* or *power sensing*. The switch also polices the power usage with the *power policing* feature.

When power policing is enabled, the switch 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 switch automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

If you do not manually configure the cutoff-power value, the switch 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 switch 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 *I_{max}* limitation and might experience an *I_{cut}* 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 switch 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 switch is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the switch has locked on it, the switch 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 switch 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 switch either turns power off to the port, or the switch generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the switch 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 switch 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 switch.

You can verify your settings by entering the **show power inline police** privileged EXEC command.

Examples

This example shows how to enable policing of the power consumption and configuring the switch to generate a syslog message on the PoE port on a switch:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# power inline police action log
```

Related Topics

[power inline](#), on page 89

[show power inline](#), on page 141

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		
<i>stack-member-number</i>		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.

Examples

This example shows how to set the power supply in slot A to off:

```
Switch> 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
Switch
```

```
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:

```
Switch> 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:

```
Switch> 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
```

Related Topics

[show env](#), on page 114

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.

```
Switch# 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 <i>stack-member-number</i> (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.
-------------------------	--

Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# 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

Related Topics

[show controllers ethernet-controller](#), on page 100

[show interfaces](#), on page 121

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		
<i>interface-id</i>	(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 <i>interface-id</i>	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 <i>if-id</i>	Specifies the Layer 3 IF interface ID for which to display port ASIC statistics.	
port-ifid <i>if-id</i>	Specifies the PortIF interface ID for which to display port ASIC statistics.	
vlan-ifid <i>if-id</i>	Specifies the VLANIF interface ID for which to display port ASIC statistics.	
switch <i>stack-member-number</i>	(Optional) Specifies the stack member number for which to display send and receive statistics.	
asic <i>asic-number</i>	(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.

Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface:

```
Switch# show controllers ethernet-controller gigabitethernet1/0/1
Transmit                               GigabitEthernet1/0/1          Receive
19216827 Total bytes                   0 Total bytes
   41935 Unicast bytes                   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
```

```
show controllers ethernet-controller
```

```
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 msec AGO

Table 6: 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.
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.

Field	Description
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.
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.

Field	Description
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 7: 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.

Field	Description
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.
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.

Field	Description
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.
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 8: 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.

Field	Description
Cos x Pause frames	The total number of class of service (CoS) x pause frames received on an interface.
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.
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:

```
Switch# 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 Register : 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
```

Related Topics

[show controllers cpu-interface](#), on page 98

show controllers utilization

To display bandwidth utilization, use the **show controllers utilization** command in EXEC mode.

show controllers [*interface-id*] **utilization**

Syntax Description	<i>interface-id</i> (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:

```
Switch> 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:

```
Switch> show controllers gigabitethernet1/0/1 utilization
Receive Bandwidth Percentage Utilization : 0
Transmit Bandwidth Percentage Utilization : 0
```

Table 9: 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.

Field	Description
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 <i>interface-id</i>	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:

```
Switch# 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:

```
Switch# 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.

```
Switch# 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:

```
Switch# 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:

```
Switch# 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 10: show eee status Field Descriptions

Field	Description
EEE (efficient-ethernet)	<p>The EEE status for the interface. This field can have any of the following values:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

Field	Description
Rx/Tx LPI Status	<p>The Low Power Idle (LPI) status for the link partner. These fields can have any of the following values:</p> <ul style="list-style-type: none">• 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. <p>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.</p>
Wake Error Count	<p>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.</p> <p>This information is useful for PHY debugging.</p>

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.
<i>stack-member-number</i>		(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.

Examples

```
Switch>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
```

```
Switch>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:

```
Switch>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:

```
Switch# 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
```

```
Switch> 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
```

```
Switch> show env temperature status
Temperature Value: 33 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 65 Degree Celsius
Red Threshold    : 75 Degree Celsius
```

Table 11: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> 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.

```
Switch> 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
```

Related Topics

[errdisable detect cause](#), on page 63

[show errdisable recovery](#), on page 119

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:

```
Switch> 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
```

Related Topics

[errdisable recovery cause](#), on page 65

[errdisable recovery interval](#), on page 68

[show errdisable detect](#), on page 117

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
<i>interface-id</i>	(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 <i>vlan-id</i>	(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 <i>number</i>	(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:

```
Switch# 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

```

Switch# **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:

Switch# **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 *interface-id* pruning** command when pruning is enabled in the VTP domain:

Switch# **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:

Switch# **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 output from the **show interfaces *interface-id* status** command:

```
Switch# 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:

```
Switch# 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:

```
Switch# show interfaces gigabitethernet1/0/2 pruning
Port Vlans pruned for lack of request by neighbor
```

```
Switch# 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
```

Related Topics

- [show interfaces counters](#), on page 125
- [show interfaces switchport](#), on page 127
- [show interfaces transceiver](#), on page 131

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	
<i>interface-id</i>	(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 <i>stack-member-number</i>	(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.

```
Switch# 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.

```
Switch# 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:

```
Switch# 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.

```
Switch# 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>

Related Topics

[show interfaces](#), on page 121

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** [{**backup** [**detail**]]**module** *number*}]

Syntax Description	
<i>interface-id</i>	(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.
backup	(Optional) Displays Flex Link backup interface configuration for the specified interface or all interfaces.
detail	(Optional) Displays detailed backup information for the specified interface or all interfaces on the switch or the stack.
module <i>number</i>	(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.

```
Switch# 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)
```

show interfaces switchport

```

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.

This is an example of output from the **show interfaces switchport backup** command:

```
Switch# show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
Gi1/0/1              Gi1/0/2              Active Up/Backup Standby
Gi3/0/3              Gi4/0/5              Active Down/Backup Up
Po1                  Po2                  Active Standby/Backup Up
```

In this example of output from the **show interfaces switchport backup** command, VLANs 1 to 50, 60, and 100 to 120 are configured on the switch:

```
Switch(config)# interface gigabitethernet 2/0/6
Switch(config-if)# switchport backup interface gigabitethernet 2/0/8
prefer vlan 60,100-120
```

When both interfaces are up, Gi2/0/8 forwards traffic for VLANs 60, 100 to 120, and Gi2/0/6 will forward traffic for VLANs 1 to 50.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
Vlans on Interface Gi 2/0/8: 60, 100-120
```

When a Flex Link interface goes down (LINK_DOWN), VLANs preferred on this interface are moved to the peer interface of the Flex Link pair. In this example, if interface Gi2/0/6 goes down, Gi2/0/8 carries all VLANs of the Flex Link pair.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Down/Backup Up
Vlans on Interface Gi 2/0/6:
Vlans on Interface Gi 2/0/8: 1-50, 60, 100-120
```

When a Flex Link interface comes up, VLANs preferred on this interface are blocked on the peer interface and moved to the forwarding state on the interface that has just come up. In this example, if interface Gi2/0/6 comes up, then VLANs preferred on this interface are blocked on the peer interface Gi2/0/8 and forwarded on Gi2/0/6.

```
Switch# show interfaces switchport backup

Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
-----
GigabitEthernet2/0/6  GigabitEthernet2/0/8  Active Up/Backup Up
Vlans on Interface Gi 2/0/6: 1-50
```

Vlans on Interface Gi 2/0/8: 60, 100-120

Related Topics

[show interfaces](#), on page 121

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	
<i>interface-id</i>	(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 <i>number</i>	(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.

Examples

This is an example of output from the **show interfaces *interface-id* transceiver properties** command:

```
Switch# show interfaces transceiver
```

```
If device is externally calibrated, only calibrated values are printed.
++ : high alarm, + : high warning, - : low warning, -- : low alarm.
NA or N/A: not applicable, Tx: transmit, Rx: receive.
mA: milliamperes, dBm: decibels (milliwatts).
```

Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Optical Tx Power (dBm)	Optical Rx Power (dBm)
Gi5/1/2	42.9	3.28	22.1	-5.4	-8.1
Te5/1/3	32.0	3.28	19.8	2.4	-4.2

```
Switch# show interfaces gigabitethernet1/1/1 transceiver properties
```

show interfaces transceiver

```
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:

```
Switch# 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.
```

Port	Temperature (Celsius)	High Alarm Threshold (Celsius)	High Warn Threshold (Celsius)	Low Warn Threshold (Celsius)	Low Alarm Threshold (Celsius)
Gi1/1/1	29.9	74.0	70.0	0.0	-4.0

Port	Voltage (Volts)	High Alarm Threshold (Volts)	High Warn Threshold (Volts)	Low Warn Threshold (Volts)	Low Alarm Threshold (Volts)
Gi1/1/1	3.28	3.60	3.50	3.10	3.00

Port	Optical Transmit Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	1.8	7.9	3.9	0.0	-4.0

Port	Optical Receive Power (dBm)	High Alarm Threshold (dBm)	High Warn Threshold (dBm)	Low Warn Threshold (dBm)	Low Alarm Threshold (dBm)
Gi1/1/1	-23.5	-5.0	-9.0	-28.2	-32.2

```
Switch# show interfaces transceiver supported-list
Transceiver Type          Cisco p/n min version
                          supporting DOM
-----
DWDM GBIC                 ALL
DWDM SFP                  ALL
RX only WDM GBIC         ALL
DWDM XENPAK               ALL
DWDM X2                   ALL
DWDM XFP                  ALL
CWDM GBIC                 NONE
CWDM X2                   ALL
CWDM XFP                  ALL
XENPAK ZR                 ALL
X2 ZR                     ALL
XFP ZR                    ALL
Rx_only_WDM_XENPAK       ALL
XENPAK_ER                 10-1888-04
X2_ER                     ALL
```

```

XFP_ER                ALL
XENPAK_LR             10-1838-04
X2_LR                 ALL
XFP_LR                ALL
XENPAK_LW             ALL
X2_LW                 ALL
XFP_LW                NONE
XENPAK_SR             NONE
X2_SR                 ALL
XFP_SR                ALL
XENPAK_LX4            NONE
X2_LX4                NONE
XFP_LX4               NONE
XENPAK_CX4            NONE
X2_CX4                NONE
XFP_CX4               NONE
SX_GBIC               NONE
LX_GBIC               NONE
ZX_GBIC               NONE
CWDM_SFP              ALL
Rx_only_WDM_SFP      NONE
SX_SFP                ALL
LX_SFP                ALL
ZX_SFP                ALL
EX_SFP                ALL
SX_SFP                NONE
LX_SFP                NONE
ZX_SFP                NONE
GigE_BX_U_SFP         NONE
GigE_BX_D_SFP         ALL
X2_LRM                ALL
SR_SFPP               ALL
LR_SFPP               ALL
LRM_SFPP              ALL
ER_SFPP               ALL
ZR_SFPP               ALL
DWDM_SFPP             ALL
GigE_BX_40U_SFP       ALL
GigE_BX_40D_SFP       ALL
GigE_BX_40DA_SFP      ALL
GigE_BX_80U_SFP       ALL
GigE_BX_80D_SFP       ALL
GIG_BXU_SFPP          ALL
GIG_BXD_SFPP          ALL
GIG_BX40U_SFPP        ALL
GIG_BX40D_SFPP        ALL
GigE_Dual_Rate_LX_SFP ALL
CWDM_SFPP             ALL
CPAK_SR10             ALL
CPAK_LR4              ALL
QSFP_LR               ALL
QSFP_SR               ALL

```

This is an example of output from the **show interfaces transceiver threshold-table** command:

```

Switch# show interfaces transceiver threshold-table
          Optical Tx      Optical Rx      Temp      Laser Bias      Voltage
          -----      -
          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

```

show interfaces transceiver

```

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>

Related Commands

Command	Description
transceiver type all	Enters the transceiver type configuration mode.
monitoring	Enables digital optical monitoring.

Related Topics

[show interfaces](#), on page 121

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 <i>stack-member-number</i> (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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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
```

Related Topics

[show mgmt-infra trace messages ilpower-ha](#), on page 137

[show mgmt-infra trace messages platform-mgr-poe](#), on page 138

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 <i>stack-member-number</i> (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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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 successfully.
```

Related Topics

[show mgmt-infra trace messages ilpower](#), on page 135

[show mgmt-infra trace messages platform-mgr-poe](#), on page 138

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 <i>stack-member-number</i> (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:

```
Switch# 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)
```

Related Topics

[show mgmt-infra trace messages ilpower](#), on page 135

[show mgmt-infra trace messages ilpower-ha](#), on page 137

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	<i>profile-number</i> (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:

```
Switch# show network-policy profile
Network Policy Profile 60
  Interface:
    none
```

Related Topics

[network-policy](#), on page 83

[network-policy profile \(global configuration\)](#), on page 84

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:

```
Switch# 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 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.	
<i>interface-id</i>	(Optional) ID of the physical interface.	
module <i>stack-member-number</i>	(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.

Examples

This is an example of output from the **show power inline** command. The table that follows describes the output fields.

```
Switch> 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
```

show power inline

```

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:

```

Switch> 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.

```

Switch> 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 12: 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: <ul style="list-style-type: none"> • 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 <i>CutoffPower</i> 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 <i>Max</i> 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 <i>AdminPowerMax</i> 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:

```
Switch> 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

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
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.

```

Switch> 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 13: 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	<p>Operating mode:</p> <ul style="list-style-type: none"> 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. <p>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.</p>
Admin Police	<p>Status of the real-time power-consumption policing feature:</p> <ul style="list-style-type: none"> 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.
Oper Police	<p>Policing status:</p> <ul style="list-style-type: none"> 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.

This is an example of output from the **show power inline priority** command on a standalone switch.

```
Switch> show power inline priority
Interface  Admin  Oper      Priority
          State  State
-----  -
Gi1/0/1   auto   off       low
Gi1/0/2   auto   off       low
Gi1/0/3   auto   off       low
Gi1/0/4   auto   off       low
Gi1/0/5   auto   off       low
Gi1/0/6   auto   off       low
Gi1/0/7   auto   off       low
Gi1/0/8   auto   off       low
Gi1/0/9   auto   off       low
```

Related Topics

[logging event power-inline-status](#), on page 79

[power inline](#), on page 89

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	<i>power-stack-name</i> (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	<p>This command is available only on switch stacks running the IP Base or IP Services image.</p> <p>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.</p>
-------------------------	---

Examples	This is an example of output from the show stack-power command:
-----------------	--

```
Switch# 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
```

Related Topics

[mode \(power-stack configuration\)](#), on page 81

[power-priority](#) , on page 87

[stack-power](#) , on page 154

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.

Examples

This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
Global Ethernet MTU is 1500 bytes.
```

Related Topics

[system mtu](#), on page 159

show tech-support poe

To display Power over Ethernet (PoE) system information, use the **show tech-support poe** command in privileged EXEC mode.

show tech-support poe

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 3.6E	This command was introduced.

Usage Guidelines The output scrolls without page breaks. Passwords and other security information are removed from the output.

This command is used for technical support.

To interrupt and terminate the show tech-support poe output, simultaneously press and release the CTRL, ALT, and 6 keys.

The show tech-support command is useful for collecting a large amount of information about your routing device for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The show tech-support command displays the output of a number of show commands at once. The output from this command varies depending on your platform and configuration. For example, access servers display voice-related show command output. Additionally, the show protocol traffic commands are displayed for only the protocols enabled on your device. For a sample display of the output of the show tech-support command, see the individual show command listed.

```
Switch#show tech-support poe
----- show clock -----
*08:41:33.103 UTC Thu Jun 7 2018
----- show version -----
Cisco IOS XE Software, Version 2018-06-05_10.29_gsiwach
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Experimental
  Version 16.9.20180604:150946 [v169_throttle-/nobackup/gsiwach/CSCvj55382 101]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 04-Jun-18 20:43 by gsiwach

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
```

GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON
 BOOTLDR: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.68, engineering software (D)

Switch uptime is 1 minute
 Uptime for this control processor is 5 minutes
 System returned to ROM by Reload Command
 System image file is "usbflash0:cat3k_caa-universalk9.2018-06-05_10.29_gsiwach.SSA.bin"
 Last reload reason: Reload Command

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

Technology-package Current	Type	Technology-package Next reboot
ipservicesk9	Smart License	ipservicesk9
None	Subscription Smart License	None

cisco WS-C3850-24P (MIPS) processor (revision P1C) with 833566K/6147K bytes of memory.
 Processor board ID FOC1808V3FZ
 2 Virtual Ethernet interfaces
 56 Gigabit Ethernet interfaces
 8 Ten Gigabit Ethernet interfaces
 2048K bytes of non-volatile configuration memory.
 4194304K bytes of physical memory.
 250456K bytes of Crash Files at crashinfo:.
 1609272K bytes of Flash at flash:.
 0K bytes of WebUI ODM Files at webui:.

.
 .
 .

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:

```
Switch# show wireless interface summary
```

speed

To specify the speed of a 10/100/1000/2500/5000 Mbps 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|2500|5000|auto} [{10|100|1000|2500|5000}]|nonegotiate}
no speed
```

Syntax Description		
	10	Specifies that the port runs at 10 Mbps.
	100	Specifies that the port runs at 100 Mbps.
	1000	Specifies that the port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mb/s ports.
	2500	Specifies that the port runs at 2500 Mbps. This option is valid and visible only on multi-Gigabit-supported Ethernet ports.
	5000	Specifies that the port runs at 5000 Mbps. This option is valid and visible only on multi-Gigabit-supported Ethernet ports.
	auto	Detects the speed at which the port should run, automatically, based on the port at the other end of the link. If you use the 10 , 100 , 1000 , 1000 , 2500 , or 5000 keyword with the auto keyword, the port autonegotiates only at the specified speeds.
	nonegotiate	Disables autonegotiation, and the port runs at 1000 Mbps.

Command Default The default is **auto**.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was modified. The following keywords were added: 2500 and 5000 . These keywords are visible only on multi-Gigabit Ethernet port supporting devices.

Usage Guidelines You cannot configure speed on 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.

The new keywords, **2500** and **5000** are visible only on multi-Gigabit (m-Gig) Ethernet supporting devices.

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 configured on each end of the link, which might 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, 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 re-enable 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.

Verify your settings using the **show interfaces** privileged EXEC command.

Examples

The following example shows how to set speed on a port to 100 Mbps:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed 100
```

The following example shows how to set a port to autonegotiate at only 10 Mbps:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10
```

The following example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# speed auto 10 100
```

Related Topics

[duplex](#), on page 61

[show interfaces](#), on page 121

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 <i>power-stack-name</i>	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 <i>stack-member-number</i>	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.

Examples

This example removes switch 2, which is connected to the power stack, from the power pool and shutting down both power ports:

```
Switch(config)# stack-power switch 2  
Switch(config-switch-stackpower)# standalone  
Switch(config-switch-stackpower)# exit
```

Related Topics

[mode \(power-stack configuration\)](#), on page 81

[power-priority](#) , on page 87

[show stack-power](#) , on page 147

switchport backup interface

To configure Flex Links, use the **switchport backup interface** command in interface configuration mode on a Layer 2 interface on the switch stack or on a standalone switch. To remove the Flex Links configuration, use the **no** form of this command.

```
switchport backup interface interface-id [{mmu primary vlan vlan-id|multicast
fast-convergence|preemption {delay seconds|mode {bandwidth|forced|off}}|prefer vlan vlan-id]
no switchport backup interface interface-id [{mmu primary vlan|multicast
fast-convergence|preemption {delay|mode}|prefer vlan}]
```

Syntax Description		
	<i>interface-id</i>	ID of the physical interface.
	mmu	(Optional) Configures the MAC move update (MMU) for a backup interface pair.
	primary vlan <i>vlan-id</i>	(Optional) VLAN ID of the primary VLAN. The range is 1 to 4094.
	multicast fast-convergence	(Optional) Configures multicast fast convergence on the backup interface.
	preemption	(Optional) Configures a preemption scheme for a backup interface pair.
	delay <i>seconds</i>	Specifies a preemption delay. The range is 1 to 300 seconds. The default is 35 seconds.
	mode	Specifies the preemption mode.
	bandwidth	Specifies that a higher bandwidth interface is preferred.
	forced	Specifies that an active interface is preferred.
	off	Specifies that no preemption occurs from backup to active.
	prefer vlan <i>vlan-id</i>	(Optional) Specifies that VLANs are carried on the backup interfaces of a Flex Link pair. VLAN ID range is 1 to 4094.

Command Default The default is to have no Flex Links defined. The preemption mode is off. No preemption occurs. Preemption delay is set to 35 seconds.

Command Modes Interface configuration

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

Usage Guidelines Flex Links are a pair of interfaces that provide backup to each other. With Flex Links configured, one link acts as the primary interface and forwards traffic, while the other interface is in standby mode, ready to begin forwarding traffic if the primary link shuts down. The interface being configured is referred to as the active link; the specified interface is identified as the backup link. The feature provides an alternative to the Spanning Tree Protocol (STP), allowing users to turn off STP and still retain basic link redundancy.

This command is available only for Layer 2 interfaces.

You can configure only one Flex Link backup link for any active link, and it must be a different interface from the active interface.

- An interface can belong to only one Flex Link pair. An interface can be a backup link for only one active link. An active link cannot belong to another Flex Link pair.
- A backup link does not have to be the same type (Fast Ethernet or Gigabit Ethernet, for instance) as the active link. However, you should configure both Flex Links with similar characteristics so that there are no loops or changes in behavior if the standby link begins to forward traffic.
- Neither of the links can be a port that belongs to an EtherChannel. However, you can configure two port channels (EtherChannel logical interfaces) as Flex Links, and you can configure a port channel and a physical interface as Flex Links, with either the port channel or the physical interface as the active link.
- If STP is configured on the switch, Flex Links do not participate in STP in all valid VLANs. If STP is not running, be sure that there are no loops in the configured topology.

This example shows how to configure two interfaces as Flex Links:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface to always preempt the backup:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption forced
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface preemption delay time:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 preemption delay 150
Switch(conf-if)# end
```

This example shows how to configure the Gigabit Ethernet interface as the MMU primary VLAN:

```
Switch# configure terminal
Switch(conf)# interface gigabitethernet1/0/1
Switch(conf-if)# switchport backup interface gigabitethernet1/0/2 mmu primary vlan 1021
Switch(conf-if)# end
```

You can verify your setting by entering the **show interfaces switchport backup** privileged EXEC command.

Related Topics

[show interfaces switchport](#), on page 127

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	<p>multicast Specifies that unknown multicast traffic should be blocked.</p> <p>Note Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.</p>				
	<p>unicast Specifies that unknown unicast traffic should be blocked.</p>				
Command Default	Unknown multicast and unicast traffic is not blocked.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th data-bbox="342 924 1101 980">Release</th> <th data-bbox="1101 924 1497 980">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="342 980 1101 1037">Cisco IOS XE 3.2SE</td> <td data-bbox="1101 980 1497 1037">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>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.</p> <p>Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.</p> <p>For more information about blocking packets, see the software configuration guide for this release.</p> <p>This example shows how to block unknown unicast traffic on an interface:</p> <pre>Switch(config-if)# switchport block unicast</pre> <p>You can verify your setting by entering the show interfaces <i>interface-id</i> switchport privileged EXEC command.</p> <p>Related Topics</p> <p>show interfaces switchport, on page 127</p>				

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	<i>bytes</i> 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.

Examples

This example shows how to set the global system MTU size to 6000 bytes:

```
Switch(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.
```

Related Topics

[show system mtu](#), on page 148

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:

```
Switch(config)# network-policy profile 1
Switch(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:

```
Switch(config)# network-policy profile 1
Switch(config-network-policy)# voice-signaling vlan 400 dscp 45
```

This example shows how to configure voice-signaling for the native VLAN with priority tagging:

```
Switch(config-network-policy)# voice-signaling vlan dot1p cos 4
```

Related Topics

[network-policy](#), on page 83

[network-policy profile \(global configuration\)](#), on page 84

[voice vlan \(network-policy configuration\)](#), on page 162

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:

```
Switch(config)# network-policy profile 1
Switch(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:

```
Switch(config)# network-policy profile 1
Switch(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:

```
Switch(config-network-policy)# voice vlan dot1p cos 4
```

Related Topics

[network-policy](#), on page 83

[network-policy profile \(global configuration\)](#), on page 84

[voice-signaling vlan \(network-policy configuration\)](#), on page 160

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 <i>interface-name</i>	Configures 10-Gigabit Ethernet interface. Values range from 0 to 9.
	Vlan <i>interface-name</i>	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:

```
Switch# wireless ap-manager interface vlan
<1-4095> Vlan interface number
```

This example shows how to configure the wireless AP-manager:

```
Switch# #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	<i>mac-addr</i>	The MAC address of the local excluded entry.
	description <i>description</i>	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:

```
Switch# 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:

```
Switch# 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 <i>size</i>	number-of-frames <i>value</i>
	Specifies the link test frame size for each packet. The values range from 1 to 1400.	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:

```
Switch# 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		
	<i>interface-name</i>	The interface number.
	TenGigabitEthernet <i>interface-name</i>	The 10-Gigabit Ethernet interface number. The values range from 0 to 9.
	Vlan <i>interface-name</i>	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:

```
Switch# 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:

```
Switch(config)# wireless peer-blocking forward-upstream TenGigabitEthernet 1/1/4
```



PART **III**

IPv6

- [IPv6 Commands](#) , on page 171



IPv6 Commands

- [ipv6 flow monitor](#) , on page 172
- [ipv6 traffic-filter](#) , on page 173
- [show wireless ipv6 statistics](#) , on page 174

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

<i>ipv6-monitor-name</i>	Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
sampler <i>ipv6-sampler-name</i>	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 (config-if)

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:

```
Switch(config)# interface gigabitethernet 1/1/2
Switch(config-if)# ip flow monitor FLOW-MONITOR-1 input
Switch(config-if)# ip flow monitor FLOW-MONITOR-2 output
Switch(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:

```
Switch(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:

```
Switch# 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 **IV**

Layer 2/3

- [Layer 2/3 Commands](#) , on page 177



Layer 2/3 Commands

- [channel-group](#), on page 179
- [channel-protocol](#), on page 182
- [clear lacp](#), on page 183
- [clear pagp](#), on page 184
- [clear spanning-tree counters](#), on page 185
- [clear spanning-tree detected-protocols](#), on page 186
- [debug etherchannel](#), on page 187
- [debug lacp](#), on page 188
- [debug pagp](#), on page 189
- [debug platform pm](#), on page 190
- [debug platform udd](#), on page 192
- [debug spanning-tree](#), on page 193
- [interface port-channel](#), on page 195
- [lacp max-bundle](#), on page 196
- [lacp port-priority](#), on page 197
- [lacp system-priority](#), on page 199
- [pagp learn-method](#), on page 200
- [pagp port-priority](#), on page 202
- [port-channel load-balance](#), on page 203
- [port-channel load-balance extended](#), on page 205
- [port-channel min-links](#), on page 206
- [show etherchannel](#), on page 207
- [show lacp](#), on page 210
- [show pagp](#), on page 214
- [show platform etherchannel](#), on page 216
- [show platform pm](#), on page 217
- [show udd](#), on page 218
- [switchport](#), on page 222
- [switchport access vlan](#), on page 224
- [switchport mode](#), on page 227
- [switchport nonegotiate](#), on page 229
- [udd](#), on page 230
- [udd port](#), on page 232

- [udld reset, on page 234](#)

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 { auto | channel-group-number mode {active|auto [non-silent]|desirable
[non-silent]|on|passive} }
no channel-group
```

Syntax Description		
auto		Enables auto-LAG feature on individual port interface. By default, the auto-LAG feature is enabled on the port.
<i>channel-group-number</i>		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 switch 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 switch or on different switches 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 switch in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode desirable:

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel on a single switch in the stack. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode active:

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/1 - 2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

This example shows how to configure a cross-stack EtherChannel in a switch 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:

```
Switch# configure terminal
Switch(config)# interface range GigabitEthernet 2/0/4 - 5
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode passive
Switch(config-if-range)# exit
Switch(config)# interface GigabitEthernet 3/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# channel-group 5 mode passive
Switch(config-if)# exit
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Topics

- [channel-protocol](#), on page 182
- [interface port-channel](#), on page 195
- [show etherchannel](#), on page 207
- [show lacp](#), on page 210
- [show pagp](#), on page 214

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

Cisco IOS XE 3.2SE

Modification

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:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

Related Topics

[channel-group](#), on page 179

[show etherchannel](#), on page 207

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	<i>channel-group-number</i> (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:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# 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.

Related Topics

[show lacp](#), on page 210

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	<i>channel-group-number</i> (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:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

You can verify that the information was deleted by entering the **show pagp** privileged EXEC command.

Related Topics

[debug pagp](#), on page 189

[show pagp](#), on page 214

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 <i>interface-id</i>	(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:

```
Switch# clear spanning-tree counters
```

Related Topics

[clear spanning-tree detected-protocols](#), on page 186

[debug spanning-tree](#), on page 193

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring switches 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 <i>interface-id</i>	(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 switch 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 switches. If a rapid-PVST+ or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the switch sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch 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 switch 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:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet2/0/1
```

Related Topics

[clear spanning-tree detected-protocols](#), on page 186

[debug spanning-tree](#), on page 193

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:

```
Switch# debug etherchannel all
```

This example shows how to display debug messages related to EtherChannel events:

```
Switch# debug etherchannel event
```

Related Topics

[show etherchannel](#), on page 207

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:

```
Switch# debug LACP all
```

This example shows how to display debug messages related to LACP events:

```
Switch# 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:

```
Switch# debug pagp all
```

This example shows how to display debug messages related to PAgP events:

```
Switch# 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:

```
Switch# debug platform pm vlans
```

debug platform udd

To enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software, use the **debug platform udd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform udd [{error|event}] [switch switch-number]
no debug platform udd [{error|event}] [switch switch-number]
```

Syntax Description	
error	(Optional) Displays error condition debug messages.
event	(Optional) Displays UDLD-related platform event debug messages.
switch <i>switch-number</i>	(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 **undebg platform udd** command is the same as the **no debug platform udd** 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 switch 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 switch 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 **undebg 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:

```
Switch# debug spanning-tree all
```

Related Topics

[clear spanning-tree counters](#), on page 185

[clear spanning-tree detected-protocols](#), on page 186

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:

```
Switch(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.

Related Topics

[channel-group](#), on page 179

[show etherchannel](#), on page 207

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	<i>max_bundle_number</i>	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 switch 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 switch (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:

```
Switch(config)# interface port-channel 2
Switch(config-if)# lACP max-bundle 5
```

Related Topics

[port-channel min-links](#), on page 206

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 switch that controls the LACP link. See the **lACP system-priority** global configuration command for determining which switch 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:

```
Switch# interface gigabitEthernet2/0/1
Switch(config-if)# lACP port-priority 1000
```

You can verify your settings by entering the **show lACP** [*channel-group-number*] **internal** privileged EXEC command.

Related Topics

[channel-group](#), on page 179

[lACP system-priority](#), on page 199

[show lACP](#), on page 210

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 switch. To return to the default setting, use the **no** form of this command.

lACP system-priority *priority*
no lACP system-priority

Syntax Description	<i>priority</i> System priority for LACP. The range is 1 to 65535.				
Command Default	The default is 32768.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

Usage Guidelines

The **lACP system-priority** command determines which switch 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 switch 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 switch (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 switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lACP system-priority** command applies to all LACP EtherChannels on the switch.

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:

```
Switch(config)# lACP system-priority 20000
```

You can verify your settings by entering the **show lACP sys-id** privileged EXEC command.

Related Topics

[channel-group](#), on page 179

[lACP port-priority](#), on page 197

[show lACP](#), on page 210

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	<p>aggregation-port Specifies address learning on the logical port channel. The switch 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.</p> <p>physical-port Specifies address learning on the physical port within the EtherChannel. The switch 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.</p>				
Command Default	The default is aggregation-port (logical port channel).				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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 switch 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 switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the switch is a physical learner, we recommend that you configure the switch 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:

```
Switch(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:

```
Switch(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.

Related Topics

[pagp port-priority](#), on page 202

[show pagp](#), on page 214

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	<i>priority</i> 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 switch 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 switch 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 switch is a physical learner, we recommend that you configure the switch 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:

```
Switch(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.

Related Topics

[pagp learn-method](#), on page 200

[port-channel load-balance](#), on page 203

[show pagp](#), on page 214

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.

Examples

This example shows how to set the load-distribution method to dst-mac:

```
Switch(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.

Examples

This example shows how to set the extended load-distribution method:

```
Switch(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	<i>min_links_number</i>	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 switch 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 switch (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:

```
Switch(config)# interface port-channel 2
Switch(config-if)# port-channel min-links 3
```

Related Topics

[lACP max-bundle](#), on page 196

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 }}] |
[ {auto|detail|load-balance |port|port-channel|protocol|summary} ]
```

Syntax Description		
<i>channel-group-number</i>	(Optional) Channel group number. The range is 1 to 128.	
auto	(Optional) Displays that Etherchannel is created automatically.	
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 auto** command:

```
switch# show etherchannel auto
Flags: D - down          P - bundled in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       U - in use       f - failed to allocate aggregator
       M - not in use, minimum links not met
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port
       A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1
```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
1      Pol(SUA)        LACP      Gi1/0/45(P) Gi2/0/21(P) Gi3/0/21(P)

```

This is an example of output from the **show etherchannel channel-group-number detail** command:

```

Switch> 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   =      PolGC = -          Pseudo port-channel = Pol
Port index     =      0Load = 0x00       Protocol = LACP

Flags: S - Device is sending Slow LACPDU      F - Device is sending fast LACPDU
      A - Device is in active mode.           P - Device is in passive mode.

Local information:
Port      Flags  State  LACP port  Admin  Oper  Port  Port
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: Pol  (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:

```

Switch> 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	Gil/0/1 (P) Gil/0/2 (P)

This is an example of output from the **show etherchannel *channel-group-number* port-channel** command:

```
Switch> 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    Gil/0/1  Active            0
  0      00    Gil/0/2  Active            0

Time since last port bundled: 01d:20h:24m:44s Gil/0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Switch# show etherchannel protocol
Channel-group listing:
-----
Group: 1
-----
Protocol: LACP
Group: 2
-----
Protocol: PAgP
```

Related Topics

- [channel-group](#), on page 179
- [channel-protocol](#), on page 182
- [interface port-channel](#), on page 195

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	
<i>channel-group-number</i>	(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 switch 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.

```
Switch> show lacp counters
          LACPDU      Marker      Marker Response      LACPDU
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 14: show lacp counters Field Descriptions

Field	Description
LACPDU Sent and Recv	The number of LACP packets sent and received by a port.

Field	Description
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:

```
Switch> 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

Port      Flags  State  LACP port  Admin  Oper  Port  Port
Port      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 15: show lacp internal Field Descriptions

Field	Description
State	State of the specific port. These are the allowed values: <ul style="list-style-type: none"> • ——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.

Field	Description
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.
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	<p>State variables for the port, encoded as individual bits within a single octet with these meanings:</p> <ul style="list-style-type: none"> • bit0: LACP_Activity • bit1: LACP_Timeout • bit2: Aggregation • bit3: Synchronization • bit4: Collecting • bit5: Distributing • bit6: Defaulted • bit7: Expired <p>Note In the list above, bit7 is the MSB and bit0 is the LSB.</p>

This is an example of output from the **show lacp neighbor** command:

```
Switch> 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:

Port      Partner          Partner          Partner
System ID 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:
```

Port	Partner System ID	Partner Port Number	Age	Partner Flags
Gi2/0/2	32768,0007.eb49.5e80	0xD	15s	SP
	LACP Partner Port Priority	Partner Oper Key	Partner Port State	
	32768	0x3	0x3C	

This is an example of output from the **show lacp sys-id** command:

```
Switch> 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.

Related Topics

[clear lacp](#), on page 183

[lacp port-priority](#), on page 197

[lacp system-priority](#), on page 199

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.

Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> 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:

```
Switch> show pagp dual-active
PAgP dual-active detection enabled: Yes
PAgP dual-active version: 1.1

Channel group 1
Port      Dual-Active   Partner      Partner   Partner
          Detect Capable Name          Port      Version
Gi1/0/1   No            Switch       Gi3/0/3   N/A
Gi1/0/2   No            Switch       Gi3/0/4   N/A

<output truncated>
```

This is an example of output from the **show pagp 1 internal** command:

```
Switch> 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

```

Port	Flags	State	Timers	Hello Interval	Partner Count	PAGP Priority	Learning Method	Group 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:

```
Switch> 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

```

Port	Partner Name	Partner Device ID	Partner Port	Age	Flags	Group Cap.
Gi1/0/1	switch-p2	0002.4b29.4600	Gi01//1	9s	SC	10001
Gi1/0/2	switch-p2	0002.4b29.4600	Gi1/0/2	24s	SC	10001

Related Topics

[clear pagp](#), on page 184

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

<i>channel-group-number</i>	Channel group number. The range is 1 to 128.
group-mask	Displays EtherChannel group mask.
load-balance	Tests EtherChannel load-balance hash algorithm.
mac <i>src-mac</i> <i>dst-mac</i>	Specifies the source and destination MAC addresses.
ip <i>src-ip</i> <i>dst-ip</i>	(Optional) Specifies the source and destination IP addresses.
port <i>src-port</i> <i>dst-port</i>	(Optional) Specifies the source and destination layer port numbers.
switch <i>switch-number</i>	(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 <i>channel-group-number</i>	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 <i>interface-id</i>		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 uddl

To display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port, use the **show uddl** command in user EXEC mode.

show uddl [**Auto-Template** | **Capwap** | **GigabitEthernet** | **GroupVI** | **InternalInterface** | **Loopback** | **Null** | **Port-channel** | **TenGigabitEthernet** | **Tunnel** | **Vlan**] *interface_number*
show uddl 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.
	<i>interface-id</i>	(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.

```
Switch> 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 16: 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:

```
Switch# 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
```

Related Topics

[uddl](#), on page 230

[uddl port](#), on page 232

[uddl reset](#), on page 234

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 switches 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.

Examples

This example shows how to cause an interface to cease operating as a Layer 2 port and become a Cisco-routed port:

```
Switch(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:

```
Switch(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 switch, use the **no** form of this command.

switchport access vlan {*vlan-id* | **name** *vlan_name*}
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.
Cisco IOS XE Denali 16.2.1	The name <i>vlan_name</i> keyword 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.

Examples

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:

```
Switch(config-if)# switchport access vlan 2
```

Examples

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 Access Mode VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Switch# configure terminal
Switch(config)# vlan 33
Switch(config-vlan)# name test
Switch(config-vlan)# end
Switch#
```

Part 2 - Checking the VLAN database

```
Switch # show vlan id 33
VLAN Name      Status   Ports
-----
```

```

33    test    active

VLAN Type  SAID      MTU    Parent RingNo BridgeNo  Stp  BrdgMode Trans1  Trans2
-----
33    enet  100033    1500   -      -      -      -      -      0      0

Remote SPAN VLAN
-----
Disabled

Primary  Secondary Type          Ports
-----

```

Part 3 - Assigning VLAN to the interface by using the name of the VLAN

```

Switch # configure terminal
Switch(config)# interface GigabitEthernet3/1/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan name test
Switch(config-if)# end
Switch#

```

Part 4 - Verifying configuration

```

Switch # show running-config interface GigabitEthernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
switchport access vlan 33
switchport mode access

```

Part 5 - Verifying interface switchport

```

Switch # show interface GigabitEthernet3/1/1 switchport
Name: Gi3/1/1
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: 33 (test)
Trunking Native Mode VLAN: 1 (default)
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: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

```

Related Topics

[switchport mode](#), on page 227

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 switches or between a switch 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



Note Although visible in the CLI, the **dot1q-tunnel** keyword is not supported.

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.

Examples

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode access
```

This example shows how set the port to dynamic desirable mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode dynamic desirable
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport mode trunk
```

Related Topics

[switchport access vlan](#), on page 224

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):

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# switchport nonegotiate
```

You can verify your setting by entering the **show interfaces interface-id switchport** privileged EXEC command.

Related Topics

[switchport mode](#), on page 227

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 <i>message-timer-interval</i>	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 Guide*, *Catalyst 2960-XR Switch Layer 2 Configuration Guide*, and *Layer 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 reenab UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenab 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:

```
Switch(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC command.

Related Topics

[show udld](#), on page 218

[udld port](#), on page 232

[udld reset](#), on page 234

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 switch.

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:

```
Switch(config)# interface gigabitethernet6/0/1  
Switch(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:

```
Switch(config)# interface gigabitethernet6/0/1  
Switch(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

Related Topics

[show udld](#), on page 218

[udld](#), on page 230

[udld reset](#), on page 234

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:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

Related Topics

[show udld](#), on page 218

[udld](#), on page 230

[udld port](#), on page 232



PART **V**

Lightweight Access Point

- [Cisco Lightweight Access Point Commands, on page 237](#)



Cisco Lightweight Access Point Commands

- [ap auth-list ap-policy](#), on page 242
- [ap bridging](#), on page 243
- [ap capwap multicast](#), on page 244
- [ap capwap retransmit](#), on page 245
- [ap capwap timers](#), on page 246
- [ap cdp](#), on page 248
- [ap core-dump](#), on page 249
- [ap country](#), on page 250
- [ap crash-file](#), on page 251
- [ap dot11 24ghz preamble](#), on page 252
- [ap dot11 24ghz dot11g](#), on page 253
- [ap dot11 5ghz channelswitch mode](#), on page 254
- [ap dot11 5ghz power-constraint](#), on page 255
- [ap dot11 beaconperiod](#), on page 256
- [ap dot11 beamforming](#), on page 257
- [ap dot11 cac media-stream](#), on page 258
- [ap dot11 cac multimedia](#), on page 261
- [ap dot11 cac video](#), on page 263
- [ap dot11 cac voice](#), on page 265
- [ap dot11 cleanair](#), on page 269
- [ap dot11 cleanair alarm air-quality](#), on page 270
- [ap dot11 cleanair alarm device](#), on page 271
- [ap dot11 cleanair device](#), on page 273
- [ap dot11 dot11n](#), on page 275
- [ap dot11 dtpc](#), on page 278
- [ap dot11 edca-parameters](#), on page 280
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 l2roam rf-params](#), on page 283
- [ap dot11 media-stream](#), on page 285
- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290

- [ap dot11 rrm logging, on page 291](#)
- [ap dot11 rrm monitor, on page 293](#)
- [ap dot11 rrm ndp-type, on page 295](#)
- [ap dot11 5ghz dot11lac frame-burst, on page 296](#)
- [ap dot1x max-sessions, on page 297](#)
- [ap dot1x username, on page 298](#)
- [ap ethernet duplex, on page 299](#)
- [ap group, on page 300](#)
- [ap image, on page 301](#)
- [ap ipv6 tcp adjust-mss, on page 302](#)
- [ap led, on page 303](#)
- [ap link-encryption, on page 304](#)
- [ap link-latency, on page 305](#)
- [ap mgmtuser username, on page 306](#)
- [ap name ap-groupname, on page 308](#)
- [ap name antenna band mode, on page 309](#)
- [ap name bhrate, on page 310](#)
- [ap name bridgegroupname, on page 311](#)
- [ap name bridging, on page 312](#)
- [ap name cdp interface, on page 313](#)
- [ap name console-redirect, on page 314](#)
- [ap name capwap retransmit, on page 315](#)
- [ap name command, on page 316](#)
- [ap name core-dump, on page 317](#)
- [ap name country, on page 318](#)
- [ap name crash-file, on page 319](#)
- [ap name dot11 24ghz rrm coverage, on page 320](#)
- [ap name dot11 49ghz rrm profile, on page 322](#)
- [ap name dot11 5ghz rrm channel, on page 324](#)
- [ap name dot11 antenna, on page 325](#)
- [ap name dot11 antenna extantgain, on page 327](#)
- [ap name dot11 cleanair, on page 328](#)
- [ap name dot11 dot11n antenna, on page 329](#)
- [ap name dot11 dual-band cleanair, on page 330](#)
- [ap name dot11 dual-band shutdown, on page 331](#)
- [ap name dot11 rrm ccx, on page 332](#)
- [ap name dot11 rrm profile, on page 333](#)
- [ap name dot11 txpower, on page 335](#)
- [ap name dot1x-user, on page 336](#)
- [ap name ethernet, on page 338](#)
- [ap name ethernet duplex, on page 339](#)
- [ap name key-zeroize , on page 340](#)
- [ap name image, on page 341](#)
- [ap name ipv6 tcp adjust-mss, on page 342](#)
- [ap name jumbo mtu, on page 343](#)
- [ap name lan, on page 344](#)

- ap name led, on page 345
- ap name link-encryption, on page 346
- ap name link-latency, on page 347
- ap name location, on page 348
- ap name mgmtuser, on page 349
- ap name mode, on page 351
- ap name monitor-mode, on page 353
- ap name monitor-mode dot11b, on page 354
- ap name name, on page 355
- ap name no dot11 shutdown, on page 356
- ap name power, on page 357
- ap name shutdown, on page 358
- ap name slot shutdown, on page 359
- ap name sniff, on page 360
- ap name ssh, on page 361
- ap name telnet, on page 362
- ap name power injector, on page 363
- ap name power pre-standard, on page 364
- ap name reset-button, on page 365
- ap name reset, on page 366
- ap name slot, on page 367
- ap name static-ip, on page 369
- ap name stats-timer, on page 370
- ap name syslog host, on page 371
- ap name syslog level, on page 372
- ap name tcp-adjust-mss, on page 373
- ap name tftp-downgrade, on page 374
- ap power injector, on page 375
- ap power pre-standard, on page 376
- ap reporting-period, on page 377
- ap reset-button, on page 378
- service-policy type control subscriber, on page 379
- ap static-ip, on page 380
- ap syslog, on page 381
- **ap name no controller** , on page 382
- ap tcp-adjust-mss size, on page 383
- ap tftp-downgrade, on page 384
- config wireless wps rogue client mse, on page 385
- clear ap name tsm dot11 all, on page 386
- clear ap config, on page 387
- clear ap eventlog-all, on page 388
- clear ap join statistics, on page 389
- clear ap mac-address, on page 390
- clear ap name wlan statistics, on page 391
- debug ap mac-address, on page 392
- show ap cac voice, on page 393

- [show ap capwap](#), on page 395
- [show ap cdp](#), on page 397
- [show ap config dot11](#), on page 398
- [show ap config dot11 dual-band summary](#), on page 399
- [show ap config fnf](#), on page 400
- [show ap config](#), on page 401
- [show ap crash-file](#), on page 402
- [show ap data-plane](#), on page 403
- [show ap dot11 l2roam](#), on page 404
- [show ap dot11 cleanair air-quality](#), on page 405
- [show ap dot11 cleanair config](#), on page 406
- [show ap dot11 cleanair summary](#), on page 408
- [show ap dot11](#), on page 409
- [show ap env summary](#), on page 415
- [show ap ethernet statistics](#), on page 416
- [show ap gps-location summary](#), on page 417
- [show ap groups](#), on page 418
- [show ap groups extended](#), on page 419
- [show ap image](#), on page 420
- [show ap is-supported](#), on page 421
- [show ap join stats summary](#), on page 422
- [show ap link-encryption](#), on page 423
- [show ap mac-address](#), on page 424
- [show ap monitor-mode summary](#), on page 426
- [show ap name auto-rf](#), on page 427
- [show ap name bhmode](#), on page 430
- [show ap name bhrate](#), on page 431
- [show ap name cac voice](#), on page 432
- [show ap name config fnf](#), on page 433
- [show ap name dot11 call-control](#), on page 434
- [show ap name cable-modem](#), on page 435
- [show ap name capwap retransmit](#), on page 436
- [show ap name ccx rm](#), on page 437
- [show ap name cdp](#), on page 438
- [show ap name channel](#), on page 439
- [show ap name config](#), on page 440
- [show ap name config dot11](#), on page 442
- [show ap name config slot](#), on page 446
- [show ap name core-dump](#), on page 450
- [show ap name data-plane](#), on page 451
- [show ap name dot11](#), on page 452
- [show ap name dot11 cleanair](#), on page 455
- [show ap name env](#), on page 456
- [show ap name ethernet statistics](#), on page 457
- [show ap name eventlog](#), on page 458
- [show ap gps-location summary](#), on page 459

- show ap name image, on page 460
- show ap name inventory, on page 461
- show ap name lan port, on page 462
- show ap name link-encryption, on page 463
- show ap name service-policy, on page 464
- show ap name tcp-adjust-mss, on page 465
- show ap name wlan, on page 466
- show ap name wlandot11 service policy, on page 468
- show ap slots, on page 469
- show ap summary, on page 470
- show ap tcp-adjust-mss, on page 471
- show ap universal summary, on page 472
- show ap uptime, on page 473
- show wireless ap summary, on page 474
- show wireless client ap, on page 475
- test ap name, on page 476
- test capwap ap name, on page 477
- trapflags ap, on page 478
- wireless probe filter, on page 479
- wireless probe limit, on page 480
- wireless wps rogue ap rldp alarm-only, on page 481
- wireless wps rogue ap rldp auto-contain, on page 482

ap auth-list ap-policy

To configure authorization policy for all Cisco lightweight access points joined to the switch, use the **ap auth-list ap-policy** command. To disable authorization policy for all Cisco lightweight access points joined to the switch, 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to enable the access point authorization policy:

```
Switch(config)# ap auth-list ap-policy authorize-ap
```

This example shows how to enable access points with locally significant certificates to connect:

```
Switch(config)# ap auth-list ap-policy lsc
```

This example shows how to enable access points with manufacture-installed certificates to connect:

```
Switch(config)# ap auth-list ap-policy mic
```

This example shows how to enable access points with self-signed certificates to connect:

```
Switch(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:

```
Switch(config)# ap bridging
```

This example shows how to disable Ethernet-to-Ethernet bridging on a lightweight access point:

```
Switch(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

<i>multicast-ip-address</i>	Multicast IP address.
service-policy	Specifies the tunnel QoS policy for multicast access points.
output	Assigns a policy map name to the output.
<i>pollicymap-name</i>	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:

```
Switch(config)# ap capwap multicast 239.2.2.2
```

This example shows how to configure a tunnel multicast QoS service policy for multicast access points:

```
Switch(config)# ap capwap multicast service-policy output tunnmulpolicy
```

Related Topics

[ap capwap retransmit](#), on page 245

[ap capwap timers](#), on page 246

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 <i>retransmit-count</i>	Specifies the access point CAPWAP control packet retransmit count. Note The count is from 3 to 8 seconds.
	interval <i>retransmit-interval</i>	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:

```
Switch# ap capwap retransmit count 3
```

This example shows how to configure the CAPWAP control packet retransmit interval for an access point:

```
Switch# 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 switch waits for an unresponsive access point to answer before considering that the access point failed to respond.
<i>seconds</i>	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 switch failure for local or all access points.
<i>seconds</i>	Small heartbeat interval (from 1 to 10 seconds) that reduces the amount of time it takes to detect a switch 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 switch. This value should be at least three times larger than the fast heartbeat timer.
<i>seconds</i>	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 switch.
<i>seconds</i>	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 switch has become unresponsive. The access point makes no further attempts to join the switch until the connection to the switch 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:

```
Switch(config)# ap capwap timers discovery-timeout 7
```

This example shows how to enable the fast heartbeat interval for all access points:

```
Switch(config)# ap capwap timers fast-heartbeat-timeout 6
```

This example shows how to configure an access point heartbeat timeout to 20:

```
Switch(config)# ap capwap timers heartbeat-timeout 20
```

This example shows how to configure the access point primary discovery request timer to 1200 seconds:

```
Switch(config)# ap capwap timers primary-discovery-timeout 1200
```

This example shows how to configure the authentication timeout to 360 seconds:

```
Switch(config)# ap capwap timers primed-join-timeout 360
```

Related Topics

[ap capwap multicast](#), on page 244

[ap capwap retransmit](#), on page 245

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

Cisco IOS XE 3.2SE

Modification

This command was introduced.

Usage Guidelines

The **no ap cdp** command disables CDP on all access points that are joined to the switch and all access points that join in the future. CDP remains disabled on both current and future access points even after the switch 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 switch, you can disable and then reenabling CDP on individual access points using the **ap name Cisco-AP cdp** command. After you disable CDP on all access points joined to the switch, you can enable and then disable CDP on individual access points.

This example shows how to enable CDP on all access points:

```
Switch(config)# ap cdp
```

This example shows how to enable CDP for Ethernet interface number 0 on all access points:

```
Switch(config)# ap cdp ethernet 0
```

Related Topics

[show ap cdp](#), on page 397

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	
<i>tftp-ip-addr</i>	IP address of the TFTP server to which the access point sends core dump files.
<i>filename</i>	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:

```
Switch(config)# ap core-dump 192.0.2.51 log compress
```

Related Topics

[ap crash-file](#), on page 251

[ap name crash-file](#), on page 319

ap country

To configure one or more country codes for a switch, 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 switch 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 switch to IN (India) and FR (France):

```
Switch(config)# ap country IN,FR
```

Related Topics

[ap name country](#), on page 318

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

Cisco IOS XE 3.2SE

Modification

This command was introduced.

This example shows how to delete all crash files:

```
Switch# ap crash-file clear-all
```

This example shows how to delete crash file 1:

```
Switch# ap crash-file delete crash-file-1
```

Related Topics

[ap name crash-file](#), on page 319

[ap name core-dump](#), on page 317

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 switch (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 switch 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 preambles:

```
Switch(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:

```
Switch(config)# ap dot11 24ghz dot11g
```

Related Topics

[show ap dot11](#), on page 409

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

Cisco IOS XE 3.2SE

Modification

This command was introduced.

This example shows how to enable the 802.11h switch announcement:

```
Switch(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	<i>value</i> 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:

```
Switch(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	5ghz	beaconperiod	time
	Specifies the settings for 2.4 GHz band.	Specifies the settings for 5 GHz band.	Specifies the beacon for a network globally.	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:

```
Switch(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:

```
Switch(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 {rate}

```

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.
<i>retryPercent</i>	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:

```
Switch(config)# ap dot11 5ghz cac media-stream multicast max-retry-percent 90
```

Related Topics

[ap dot11 cac multimedia](#), on page 261

[ap dot11 cac video](#), on page 263

[ap dot11 cac voice](#), on page 265

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.
	<i>bandwidth</i>	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:

```
Switch(config)# ap dot11 5ghz cac multimedia max-bandwidth 5
```

Related Topics

[ap dot11 cac media-stream](#), on page 258

[ap dot11 cac video](#), on page 263

[ap dot11 cac voice](#), on page 265

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.
<i>value</i>		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.
<i>value</i>		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:

```
Switch(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:

```
Switch(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:

```
Switch(config)# ap dot11 24ghz cac video roam-bandwidth 10
```

Related Topics

[ap dot11 cac media-stream](#), on page 258

[ap dot11 cac multimedia](#), on page 261

[ap dot11 cac voice](#), on page 265

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.
<i>value</i>	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.
<i>value</i>	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.

<i>bw</i>	Bandwidth in kbps. The following bandwidth values specify parameters for the SIP codecs: <ul style="list-style-type: none"> • 64kbps—Specifies CAC parameters for the SIP G711 codec. • 8kbps—Specifies CAC parameters for the SIP G729 codec. <p>Note The default value is 64 Kbps.</p>
sample-interval	Specifies the packetization interval for SIP codec.
<i>value</i>	Packetization interval in msec. 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.
<i>x</i>	Stream size. The range of the stream size is from 84000 to 92100.
max-streams	Specifies the maximum number of streams per TSPEC.
<i>y</i>	Number (1 to 5) of voice streams. <p>Note The default number of streams is 2 and the mean data rate of a stream is 84 kbps.</p>
tspec-inactivity-timeout	Specifies TSPEC inactivity timeout processing mode. <p>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.</p>
enable	Processes the TSPEC inactivity timeout messages.
ignore	Ignores the TSPEC inactivity timeout messages. <p>Note The default is ignore (disabled).</p>

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:

```
Switch(config)# ap dot11 24ghz cac voice acm
```

This example shows how to enable the load-based CAC on the voice access category:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(config)# ap dot11 24ghz cac voice tspec-inactivity-timeout enable
```

Related Topics

[ap dot11 cac media-stream](#), on page 258

[ap dot11 cac multimedia](#), on page 261

[ap dot11 cac video](#), on page 263

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:

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

Related Topics

[ap dot11 cleanair alarm air-quality](#), on page 270

[ap dot11 cleanair alarm device](#), on page 271

[ap dot11 cleanair device](#), on page 273

[ap name dot11 dual-band cleanair](#), on page 330

[ap name dot11 dual-band shutdown](#), on page 331

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.
	<i>value</i>	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:

```
Switch(config)# ap dot11 24ghz cleanair air-quality threshold 90
```

Related Topics

- [ap dot11 cleanair](#), on page 269
- [ap dot11 cleanair alarm device](#), on page 271
- [ap dot11 cleanair device](#), on page 273

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|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:

```
Switch(config)# no ap dot11 24ghz cleanair alarm device zigbee
```

This example shows how to enable alarms for detection of Bluetooth links:

```
Switch(config)# ap dot11 24ghz cleanair alarm device bt-link
```

Related Topics

[ap dot11 cleanair alarm air-quality](#), on page 270

[ap dot11 cleanair](#), on page 269

[ap dot11 cleanair device](#), on page 273

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 switch to monitor ZigBee interferences:

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

Related Topics

[ap dot11 cleanair alarm air-quality](#), on page 270

[ap dot11 cleanair](#), on page 269

[ap dot11 cleanair alarm device](#), on page 271

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.
<i>priority_value</i>	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.
<i>priority_value</i>	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.
<i>scheduler_value</i>	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.
<i>rate</i>	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:

```
Switch(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:

```
Switch(config)# ap dot11 24ghz dot11n a-msdu tx priority all
```

This example shows how to enable only long guard intervals:

```
Switch(config)# ap dot11 24ghz dot11n guard-interval long
```

This example shows how to specify MCS rates:

```
Switch(config)# ap dot11 24ghz dot11n mcs tx 5
```

This example shows how to enable RIFS:

```
Switch(config)# ap dot11 24ghz dot11n rifs rx
```

Related Topics

[ap dot11 dtpc](#), on page 278

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 be used when the network is disabled using the ap dot11 {24ghz 5ghz} shutdown command.
<i>threshold</i>		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 switch configures all joining access points for this feature.

This example shows how to enable DTPC for the 5 GHz band:

```
Switch(config)# ap dot11 5ghz dtpc
```

This example shows how to enable the CCX expedited bandwidth settings:

```
Switch(config)# ap dot11 5ghz exp-bwreq
```

This example shows how to configure the fragmentation threshold on the 5 GHz band with the threshold number of 1500 bytes:

```
Switch(config)# ap dot11 5ghz fragmentation 1500
```

Related Topics

[ap dot11 beaconperiod](#), on page 256

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:

```
Switch(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 switch 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:

```
Switch(config)# ap dot11 5ghz rrm group-mode auto
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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.
	<i>value</i>	Sensitivity value. You can specify any one of the following three optional sensitivity values: <ul style="list-style-type: none"> • 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:

```
Switch(config)# ap dot11 24ghz rrm channel cleanair-event sensitivity high
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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.
	<i>min-rssi</i>	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.
	<i>roam-hyst</i>	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.
	<i>scan-thresh</i>	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.
	<i>trans-time</i>	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		
	<i>min-rssi</i>	-85
	<i>roam-hyst</i>	2
	<i>scan-thresh</i>	-72
	<i>trans-time</i>	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:

```
Switch(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 <i>value</i>		Specifies the maximum number of streams allowed on a client.
radio-maximum <i>value</i>		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:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(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 {disableinterval}
```

Syntax Description	24ghz	Specifies the 2.4-GHz band.
	5ghz	Specifies the 5-GHz band.
	disable	Disables support for CCX client location measurements.
	<i>interval</i>	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:

```
Switch(config)# no ap dot11 24ghz rrm ccx location-measurement
```

Related Topics

- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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.
<i>channel_number</i>		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.
<i>value</i>		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.
<i>value</i>		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.
<i>value</i>		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 17: DCA Sensitivity Threshold

Sensitivity	2.4 Ghz DCA Sensitivity Threshold	5 Ghz DCA Sensitivity Threshold
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

This example shows how to configure the switch to start running DCA at 5 pm for the 2.4 GHz band:

```
Switch(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:

```
Switch(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:

```
Switch(config)# ap dot11 24ghz rrm channel dca sensitivity low
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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.
	<i>controller-name</i>	Name of the switch to be added.
	<i>controller-ip</i>	IP address of the switch 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 switch in the 5 GHz band RF group:

```
Switch(config)# ap dot11 5ghz rrm group-member cisco-controller 192.0.2.54
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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:

```
Switch(config)# ap dot11 5ghz rrm logging channel
```

This example shows how to turn the 5 GHz coverage profile violation logging selection mode on:

```
Switch(config)# ap dot11 5ghz rrm logging coverage
```

This example shows how to turn the 5 GHz foreign interference profile violation logging selection mode on:

```
Switch(config)# ap dot11 5ghz rrm logging foreign
```

This example shows how to turn the 5 GHz load profile logging mode on:

```
Switch(config)# ap dot11 5ghz rrm logging load
```

This example shows how to turn the 5 GHz noise profile logging mode on:

```
Switch(config)# ap dot11 5ghz rrm logging noise
```

This example shows how to turn the 5 GHz performance profile logging mode on:

```
Switch(config)# ap dot11 5ghz rrm logging performance
```

This example shows how to turn the 5 GHz transmit power change mode on:

```
Switch(config)# ap dot11 5ghz rrm logging txpower
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm monitor](#), on page 293
- [ap dot11 rrm ndp-type](#), on page 295

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.	
rsi-normalization	Configure RRM Neighbor Discovery RSSI Normalization.	
<i>seconds</i>	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:

```
Switch(config)# ap dot11 24ghz rrm monitor channel-list country
```

This example shows how to set the coverage measurement interval to 60 seconds:

```
Switch(config)# ap dot11 24ghz rrm monitor coverage 60
```

Related Topics

[ap dot11 rrm ccx location-measurement](#), on page 287

[ap dot11 rrm channel cleanair-event](#), on page 282
[ap dot11 rrm channel dca](#), on page 288
[ap dot11 rrm group-member](#), on page 290
[ap dot11 rrm logging](#), on page 291
[ap dot11 rrm group-mode](#), on page 281
[ap dot11 rrm ndp-type](#), on page 295

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:

```
Switch(config)# ap dot11 5ghz rrm ndp-type protected
```

Related Topics

- [ap dot11 rrm ccx location-measurement](#), on page 287
- [ap dot11 rrm channel cleanair-event](#), on page 282
- [ap dot11 rrm channel dca](#), on page 288
- [ap dot11 rrm group-member](#), on page 290
- [ap dot11 rrm logging](#), on page 291
- [ap dot11 rrm group-mode](#), on page 281
- [ap dot11 rrm monitor](#), on page 293

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.

```
Switch# ap 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	<i>num-of-sessions</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>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.</p> <p>This example shows how to configure the maximum number of simultaneous 802.1X sessions:</p> <pre>Switch(config)# ap dot1x max-sessions 100</pre>				

ap dot1x username

To configure the 802.1X username and password for all access points that are currently joined to the switch and any access points that join the switch 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 switch, 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		
	<i>user-id</i>	Username.
	password	Specifies an 802.1X password for all access points.
	0	Specifies an unencrypted password.
	8	Specifies an AES encrypted password.
	<i>password_string</i>	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:

```
Switch(config)# ap dot1x username cisco123 password 0 cisco2020
```

Related Topics

[show ap summary](#), on page 470

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 ap ethernet** form of this command.

```
ap ethernet duplex duplex speed speed
no ap ethernet
```

Syntax Description	<i>duplex</i>	Ethernet port duplex settings. You can specify the following options to configure the duplex settings: <ul style="list-style-type: none"> • 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.
	<i>speed</i>	Ethernet port speed settings. You can specify the following options to configure the speed settings: <ul style="list-style-type: none"> • 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:

```
Switch(config)# ap ethernet duplex full speed 1000
```

Related Topics

[show ap summary](#), on page 470

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	<i>group-name</i> 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:

```
Switch(config)# ap group sampleapgroup
```

Related Topics

[ap name ap-groupname](#), on page 308

ap image

To configure an image on all access points that are associated to the switch, 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:

```
Switch# ap image predownload
```

This example shows how to reboot all access points:

```
Switch# ap image reset
```

This example shows how to swap the access point's primary and secondary images:

```
Switch# ap image swap
```

Related Topics

[show ap image](#), on page 420

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.
<i>size</i>	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:

```
Switch(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:

```
Switch(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:

```
Switch(config)# ap link-encryption
```

Related Topics

[ap link-latency](#), on page 305

ap link-latency

To enable link latency for all access points that are currently associated to the switch, use the **ap link-latency** command. To disable link latency all access points that are currently associated to the switch, 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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 switch. 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:

```
Switch(config)# ap link-latency
```

Related Topics

[ap link-encryption](#), on page 304

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	<i>username</i>	Specifies the username for access point management.
password	<i>password</i>	Specifies the password for access point management.
password_type	<i>password_type</i>	Password type. You can specify any one of the following two password types: <ul style="list-style-type: none"> • 0—Specifies that an unencrypted password will follow. • 8—Specifies that an AES encrypted password will follow.
password	<i>password</i>	Access point management password. <p>Note The password does not get encrypted by service-password encryption.</p>
secret	<i>secret</i>	Specifies the secret password for privileged access point management.
secret_type	<i>secret_type</i>	Secret type. You can specify any one of the following two secret types: <ul style="list-style-type: none"> • 0—Specifies that an unencrypted secret password will follow. • 8—Specifies that an AES encrypted secret password will follow.
secret	<i>secret</i>	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 l, |, 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:

```
Switch(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	<i>ap-name</i>	Name of the Cisco lightweight access point.
	<i>group-name</i>	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:

```
Switch# ap name AP01 ap-groupname superusers
```

Related Topics

[ap group](#), on page 300

[show ap summary](#), on page 470

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	<i>ap-name</i>	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.

```
Switch# ap 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	<i>ap-name</i>	Name of the Cisco access point.
	<i>kbps</i>	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:

```
Switch# 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:

```
Switch# ap name AP02 bridgegroupname West
```

This example shows how to delete a bridge group name on Cisco access point's bridge group name AP02:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# ap name TSIM_AP2 bridging
```

Related Topics

[ap bridging](#), on page 243

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	<i>ap-name</i>	Name of the Cisco lightweight access point.
	ethernet	Enables CDP on an Ethernet interface.
	<i>ethernet-id</i>	Ethernet interface number from 0 to 3.
	radio	Enables CDP for a radio interface.
	<i>radio-id</i>	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 switch, you can disable and then reenable CDP on individual access points by using the ap name <i>ap-name</i> cdp interface ethernet <i>ethernet-id</i> cisco_ap command. After you disable CDP on all access points that are joined to the switch, 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:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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	
<i>ap-name</i>	Name of the Cisco lightweight access point.
count	Sets the number of times control packet will be retransmitted.
<i>count-value</i>	Number of times that the control packet will be retransmitted from 3 to 8.
interval	Sets the control packet retransmission timeout interval.
<i>interval-time</i>	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:

```
Switch# ap name AP01 capwap retransmit interval 5
```

This example shows how to configure the retransmission retry count for a specific access point:

```
Switch# 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:

```
Switch# 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	
<i>ap-name</i>	Name of the access point.
<i>tftp-ip-addr</i>	IP address of the TFTP server to which the access point sends core dump files.
<i>filename</i>	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:

```
Switch# ap name AP2 core-dump 192.1.1.1 log compress
```

Related Topics

[ap core-dump](#), on page 249

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	
<i>ap-name</i>	Name of the Cisco lightweight access point.
<i>country-code</i>	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 switches 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:

```
Switch# ap name AP2 country JP
```

Related Topics

[ap country](#), on page 250

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

<i>ap-name</i>	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:

```
Switch# 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:

```
Switch# ap name AP02 crash-file get-radio-core-dump slot 0
```

Related Topics

[ap crash-file](#), on page 251

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 switch 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 switch 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 switch 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:

```
Switch# 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:

```
Switch# ap name AP2 dot11 24ghz rrm coverage level 60
```

Related Topics

[ap name dot11 49ghz rrm profile](#), on page 322

[ap name dot11 5ghz rrm channel](#), on page 324

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** *value*|**utilization** *value*}

Syntax Description

ap-name	Name of the Cisco lightweight access point.
clients	Sets the access point client threshold.
<i>value</i>	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 <i>value</i>	Sets the 802.11a Cisco access point coverage exception level from 0 to 100 percent.
foreign	Sets the foreign 802.11 transmitter interference threshold.
<i>value</i>	Foreign 802.11 transmitter interference threshold from 0 to 100 percent. Note The default is 10 percent.
level <i>value</i>	Sets the 802.11a Cisco access point client minimum exception level from 1 to 75 clients.
noise	Sets the 802.11 foreign noise threshold.
<i>value</i>	802.11 foreign noise threshold from -127 to 0 dBm. Note The default is -70 dBm.
throughput	Sets the data-rate throughput threshold.
<i>value</i>	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.
<i>value</i>	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:

```
Switch# 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:

```
Switch# ap name AP1 dot11 49ghz rrm profile customize
```

This example shows how to set the foreign transmitter interference threshold for AP1 to 0 percent:

```
Switch# ap name AP1 dot11 49ghz rrm profile foreign 0
```

This example shows how to set the foreign noise threshold for AP1 to 0 dBm:

```
Switch# 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:

```
Switch# ap name AP1 dot11 49ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Switch# ap name AP1 dot11 49ghz rrm profile utilization 100
```

Related Topics

[ap name dot11 24ghz rrm coverage](#), on page 320

[ap name dot11 5ghz rrm channel](#), on page 324

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	
	<i>ap-name</i> Name of the Cisco lightweight access point.
	<i>channel</i> 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:

```
Switch# ap name AP01 dot11 5ghz rrm channel 140
```

Related Topics

- [ap name dot11 24ghz rrm coverage](#), on page 320
- [ap name dot11 49ghz rrm profile](#), on page 322

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		
<i>ap-name</i>	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.
<i>gain</i>	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:

```
Switch# 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:

```
Switch# 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:

```
Switch# ap name AP02 dot11 24ghz antenna selection interval
```

Related Topics

[ap name dot11 antenna extantgain](#), on page 327

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	<i>ap-name</i>	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.
	<i>gain</i>	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:

```
Switch# ap name AP1 dot11 49ghz antenna extantgain 0.5
```

Related Topics

[ap name dot11 antenna](#), on page 325

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

Cisco IOS XE 3.2SE

Modification

This command was introduced.

This example shows how to enable CleanAir on the 2.4 GHz band:

```
Switch# 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

<i>ap-name</i>	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:

```
Switch# ap name AP02 dot11 5ghz dot11n antenna B
```

This example shows how to disable antenna C on access point AP02:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# ap name AP01 dot11 dual-band cleanair
```

Related Topics

- [ap name dot11 dual-band shutdown](#), on page 331
- [show ap dot11 cleanair config](#), on page 406
- [show ap name config dot11](#), on page 442

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	<i>ap-name</i> Name of the Cisco AP.				
	shutdown Disables the dual band radio on the Cisco AP.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
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:

```
Switch# 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		
	<i>ap-name</i>	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.
	<i>interval</i>	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:

```
Switch# ap name AP01 dot11 24ghz rrm ccx location-measurement 3200
```

Related Topics

[ap name dot11 rrm profile](#), on page 333

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	
<i>ap-name</i>	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.
<i>value</i>	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.
<i>value</i>	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.
<i>value</i>	802.11 foreign noise threshold between -127 and 0 dBm. Note The default is -70 dBm.
throughput	Sets the data-rate throughput threshold.
<i>value</i>	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.
<i>value</i>	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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# ap name AP1 dot11 5ghz rrm profile throughput 10000000
```

This example shows how to set the RF utilization threshold for AP1 to 100 percent:

```
Switch# ap name AP1 dot11 5ghz rrm profile utilization 100
```

Related Topics

[ap name dot11 rrm ccx](#), on page 332

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 {autopower-level}}
```

Syntax Description	
<i>ap-name</i>	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.
<i>power-level</i>	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:

```
Switch# ap name AP1 dot11 24ghz txpower auto
```

Related Topics

[show ap config dot11](#), on page 398

ap name dot1x-user

To configure the global authentication username and password for an access point that is currently joined to the switch, 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	
<i>ap-name</i>	Name of the access point.
global-override	Forces the access point to use the switch's global authentication settings.
username	Specifies to add a username.
<i>user-id</i>	Username.
password	Specifies to add a password.
<i>passwd</i>	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:

```
Switch# ap name AP02 dot1x-user username Cisco123 password Cisco2020
```

This example shows how to disable the authentication for access point cisco_ap1:

```
Switch# ap name cisco_ap1 no dot1x-user
```

Related Topics

[show ap summary](#), on page 470

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		
<i>ap-name</i>	Name of the Cisco lightweight access point.	
<i>intf-number</i>	Ethernet interface number from 0 to 3.	
mode	Configures access or trunk mode.	
access	Configures the port in access mode.	
<i>vlan-id</i>	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.

```
Switch# 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	
<i>ap-name</i>	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:

```
Switch# ap name AP2 ethernet duplex full 1000
```

Related Topics

[show ap summary](#), on page 470

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	<i>ap- name</i>	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.

```
Switch# ap 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	<i>ap-name</i>	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:

```
Switch# ap name AP2 image predownload
```

This example shows how to swap an access point's primary and secondary images:

```
Switch# ap name AP2 image swap
```

Related Topics

[show ap image](#), on page 420

[ap image](#), on page 301

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	
<i>ap-name</i>	Name of the Cisco AP.
adjust-mss	Configures IPv6 TCP MSS settings for all Cisco APs.
<i>size</i>	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:

```
Switch# 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	<i>ap-name</i>	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.

```
Switch# ap 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.
	<i>port-id</i>	The ID of the port. The range is 1-4
	shutdown	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:

```
Switch# 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:

```
Switch# ap name AP2 led
```

This example shows how to disable the LED state for an access point:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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 switch, use the **ap name link-latency** command. To disable link latency for a specific Cisco lightweight access point that is currently associated to the switch, use the **no** form of this command.

```
ap name ap-name link-latency
ap name ap-name no link-latency
```

Syntax Description	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	Link latency is disabled by default.				
Command Modes	Any command mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>This command enables or disables link latency only for access points that are currently joined to the switch. It does not apply to access points that join in the future.</p> <p>This example shows how to enable link latency on access points:</p> <pre>Switch# ap name AP2 link-latency</pre>				

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

Cisco IOS XE 3.2SE

Modification

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:

```
Switch# ap name AP1 location Building1
```

Related Topics

[show ap summary](#), on page 470

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 switch'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

<i>ap-name</i>	Name of the Cisco lightweight access point.
username	Specifies the username for access point management.
<i>username</i>	Management username.
password	Specifies the password for access point management.
<i>password</i>	Access point management password.
secret	Specifies the secret password for privileged access point management.
<i>secret</i>	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 l, |, 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:

ap name mgmtuser

```
Switch# ap name AP01 mgmtuser username acd password Arc_1234 secret Mid_1234
```

ap name mode

To change a Cisco switch 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		
	<i>ap-name</i>	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 switch to communicate with access point AP01 in local mode:

```
Switch# ap name AP01 mode local submode none
```

This example shows how to set the switch to communicate with access point AP01 in a wired rogue access point detector mode:

```
Switch# ap name AP01 mode rogue
```

This example shows how to set the switch to communicate with access point AP02 in wireless sniffer mode:

```
Switch# ap name AP02 mode sniffer
```

Related Topics

[show ap monitor-mode summary](#), on page 426

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

<i>ap-name</i>	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:

```
Switch# ap name AP01 monitor-mode wips
```

Related Topics

[show ap monitor-mode summary](#), on page 426

[show ap config](#), on page 401

ap name monitor-mode dot11b

To configure 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

<i>ap-name</i>	Name of the access point.
fast-channel	Specifies the 2.4 GHz band scanning channel (or channels) for a monitor-mode access point.
<i>channel1</i>	Scanning channel1.
<i>channel2</i>	(Optional) Scanning channel2.
<i>channel3</i>	(Optional) Scanning channel3.
<i>channel4</i>	(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:

```
Switch# ap name AP01 monitor-mode dot11b fast-channel 1 6 11
```

Related Topics

[show ap monitor-mode summary](#), on page 426

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:

```
Switch# ap name AP1 name AP2
```

Related Topics

[show ap config](#), on page 401

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	<i>ap-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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	
<i>ap-name</i>	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:

```
Switch# ap name AP01 power injector
```

This example shows how to enable the inline power Cisco prestandard switch state for access point AP02:

```
Switch# 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	<i>ap-name</i> 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 a specific Cisco lightweight access point:

```
Switch# 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

<i>ap-name</i>	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:

```
Switch# 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		
<i>ap-name</i>	Name of the Cisco lightweight access point.	
dot11a	Specifies the 2.4 GHz band.	
dot11b	Specifies the 5 GHz band.	
<i>channel</i>	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.	
<i>server-ip-address</i>	IP address of the remote machine running Omnippeek, Airoppeek, 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 Omnippeek, Airoppeek, 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:

```
Switch# 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	<i>ap-name</i> 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 switch 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:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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		
	<i>ap-name</i>	Name of the 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.
	<i>switch-MAC-address</i>	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:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# ap name AP02 power pre-standard
```

This example shows how to disable the inline power Cisco prestandard switch state for access point AP02:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to enable the Reset button for access point AP03:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to reset a Cisco lightweight access point named AP2:

```
Switch# ap name AP2 reset
```

Related Topics

[show ap config](#), on page 401

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 {globalchannel-level}}
ap name ap-name no slot {0|1|2|3} shutdown
```

Syntax Description					
<i>ap-name</i>	Name of the Cisco access point.				
<i>slot-number</i>	Slot downlink radio to which the channel is assigned. You can specify the following slot numbers: <ul style="list-style-type: none"> • 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.				
<i>channel-number</i>	Channel number from 1 to 169.				
width	Specifies the channel width for the slot.				
<i>channel-width</i>	Channel width from 20 to 40.				
rtsthreshold	Specifies the RTS/CTS threshold for an access point.				
<i>value</i>	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.				
<i>channel-level</i>	Transmit power level for the slot from 1 to 7.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to enable slot 3 for the access point abc:

```
Switch# ap name abc slot 3
```

This example shows how to configure RTS for the access point abc:

```
Switch# 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		
	<i>ap-name</i>	Name of the access point.
	domain	Specifies the Cisco access point domain name.
	<i>domain-name</i>	Domain to which a specific access point belongs.
	ip-address	Specifies the Cisco access point static IP address.
	<i>ip-address</i>	Cisco access point static IP address.
	netmask	Specifies the Cisco access point static IP netmask.
	<i>netmask</i>	Cisco access point static IP netmask.
	gateway	Specifies the Cisco access point gateway.
	<i>gateway</i>	IP address of the Cisco access point gateway.
	nameserver	Specifies a DNS server so that a specific access point can discover the switch using DNS resolution.
	<i>ip-address</i>	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 switch 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:

```
Switch# 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 switch, use the **ap name stats-timer** command.

ap name *ap-name* **stats-timer** *timer-value*

Syntax Description	
	<i>ap-name</i> Name of the Cisco lightweight access point.
	<i>timer-value</i> 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:

```
Switch# 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	
<i>ap-name</i>	Name of the Cisco lightweight access point.
<i>syslog-host-ip-address</i>	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:

```
Switch# ap name AP2 syslog host 192.0.2.54
```

Related Topics

[ap syslog](#), on page 381

[show ap config](#), on page 401

[show ap name config](#), on page 440

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		
	<i>ap-name</i>	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:

```
Switch# 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	<i>ap-name</i>	Name of the access point.
	<i>size</i>	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:

```
Switch# ap name ciscoap tcp-adjust-mss size 1200
```

Related Topics

[show ap name tcp-adjust-mss](#), on page 465

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	<i>ap-name</i>	Name of the Cisco lightweight access point.
	<i>tftp-server-ip</i>	IP address of the TFTP server.
	<i>filename</i>	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:

```
Switch# 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 switch, 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.
	<i>switch-MAC-address</i>	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 switch:

```
Switch(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 switch 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	<i>value</i> Time period in seconds from 10 to 120.				
Command Default	None				
Command Modes	Global configuration				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example show how to configure the access point rogue/error reporting:

```
Switch(config)# ap reporting-period 100
```

This example show how to disable the access point rogue/error reporting:

```
Switch(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 switch, 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:

```
Switch(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-policy type control subscriber *<subscriber-policy-name>*

Syntax Description	service-policy Instructs the access point to apply global subscriber control policy.				
	<i><subscriber-policy-name></i> Name of the subscriber policy.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				

Example

This example shows how to disable the global subscriber control policy.

```
Switch#no 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.
	<i>domain-name</i>	Domain name.
	name-server	Specifies a DNS server so that a specific access point or all access points can discover the switch using DNS resolution.
	<i>ip-address</i>	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 switch 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:

```
Switch(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 switch, 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 switch.
	<i>ipaddress</i>	IP address of the syslog server.
	level	Specifies the system logging level for all the access points joined to the switch.
	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 switch. 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:

```
Switch(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		
	<i>ap- name</i>	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 unconfigure the primary and configure the secondary controller.

Example

This example shows how to unconfigure the primary controller.

```
Switch# ap 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	<i>size</i> Maximum segment size, from 536 to 1363 bytes.				
Command Default	None				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch(config)# ap tcp-adjust-mss 1200
```

Related Topics

[show ap name tcp-adjust-mss](#), on page 465

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	
<i>tftp-server-ip</i>	IP address of the TFTP server.
<i>filename</i>	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:

```
Switch(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	Command	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.

```
Switch#wireless 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

<i>ap-name</i>	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:

```
Switch# 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	<i>ap-name</i>	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 switch.
	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:

```
Switch# clear ap config AP01
```

Related Topics

[show ap config](#), on page 401

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:

```
Switch# 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:

```
Switch# 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	<i>mac</i>	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:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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	<i>mac-address</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>10.3Cisco IOS XE 3.3 SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	10.3Cisco IOS XE 3.3 SE	This command was introduced.
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 :

```
Switch# debug ap mac-address
ap mac-address debugging is on
```

This example shows how to disable debugging mac-address on an AP :

```
Switch# 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
--	-------	---------	-----------	-----------	----------

```
show ap cac voice
```

```
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 switch.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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 switch:

```
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 switch, 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:

```
Switch# show ap cdp
```

This example shows how to display details about all neighbors that are using CDP:

```
Switch# show ap cdp neighbors
```

Related Topics

[ap cdp](#), on page 248

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:

```
Switch# 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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
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 switch, 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to display global syslog server settings:

```
Switch# 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:

```
Switch# show ap crash-file
```

Related Topics

[ap crash-file](#), on page 251

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:

```
Switch# 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 <i>mac-address</i> 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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 switch.

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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```

Switch# 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:

```

Switch# 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:

```

Switch# 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:

```

Switch# 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:

```
Switch# 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 Admission Control (CAC) configuration
    Voice AC
      Voice AC - Admission control (ACM) : Disabled
      Voice Stream-Size : 84000
      Voice Max-Streams : 2
      Voice Max RF Bandwidth : 75
      Voice Reserved Roaming Bandwidth : 6
      Voice Load-Based CAC mode : Enabled
      Voice tspec inactivity timeout : Enabled
    CAC SIP-Voice configuration
      SIP based CAC : Disabled
      SIP call bandwidth : 64
      SIP call bandwidth sample-size : 20
    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:

```

Switch# 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:

```

Switch# show ap dot11 5ghz service-policy

```

This example shows how to display a summary of the 802.11b access point settings:

```

Switch# 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:

```
Switch# 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:

```
Switch# show ap dot11 5ghz ccx global
802.11a Client Beacon Measurements:
  disabled
```

Related Topics

[ap dot11 rrm channel dca](#), on page 288

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:

```
Switch#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

This command has no keywords and arguments.

Command Default

None

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 Ethernet statistics for all access points:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
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:

```
Switch# 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	<i>model-part-number</i> Part number of the AP model. For example, AIR-LAP1142N-N-K9.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.7.0E</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.7.0E	This command was introduced.
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:

```
Switch# 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:

```
Switch# 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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example show how to display the link-encryption status:

```
Switch# 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	
<i>mac-address</i>	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 switch:

```
Switch# 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 to the AP has reached maximum : Number of message retransmission
Last join error summary
  Type of error that occurred last : AP got or has been disconnected
Reason for error that occurred last to the AP has reached maximum : Number of message retransmission
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:

```
Switch# 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:

```
Switch# 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					
<i>ap-name</i>	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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to display auto-RF information for an access point:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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
2	1	802.11a	0	23437	0

```
Wired Bandwidth (in Kbps)
```

Slot#	Wlan-ID	Wlan-Name	BW-Config	BW-Avail
1	0	1	maria-open	0
2	0	12	24	0
3	1	1	maria-open	0
4	1	12	24	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	<i>ap-name</i> 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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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	
<i>ap-name</i>	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:

```
Switch# 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	<i>ap-name</i> Name of the specific AP.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.7.0 E</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.7.0 E	This command was introduced.
Release	Modification				
Cisco IOS XE 3.7.0 E	This command was introduced.				

This example shows how to show AP CAPWAP CCX on AP1:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to display CAPWAP retransmit settings of an access point:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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	<i>ap-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to display CDP information for an access point:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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:

```
Switch# show ap name AP01 config ethernet
```

```
VLAN Tagging Information for AP01
```

This example shows how to display common information for an access point:

```
Switch# 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 : Tel1/0/1
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	
<i>ap-name</i>	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:

```
Switch# 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            : Tel1/0/1
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 Update 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	<i>ap-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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            : Tel/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

```

show ap name config slot

```

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	<i>ap-name</i> 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:

```
Switch# 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
```

Related Topics

[ap name core-dump](#), on page 317

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	<i>ap-name</i> 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:

```
Switch# show ap name AP01 data-plane
```

AP Name	Min Data Round Trip	Data Round Trip	Max Data Round Trip	Last 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-policy output|stats|tsm
{allclient-mac}}
```

Syntax Description		
	<i>ap-name</i>	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.
	<i>client-mac</i>	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:

```
Switch# 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:

```
Switch# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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 insufficient 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:

```
Switch# show ap name AP01 dot11 24ghz tsm all
```


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	<i>ap-name</i> Name of the specific AP.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.7.0 E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.7.0 E	This command was introduced.
Release	Modification				
Cisco IOS XE 3.7.0 E	This command was introduced.				

This example shows how to show AP environment on AP1:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.
---------------------------	--

Command Default	None.
------------------------	-------

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 Ethernet statistics of an access point:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# 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:

```
Switch# 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.
<i>port-id</i>	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:

```
Switch# 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	<i>ap-name</i> 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:

```
Switch# show ap name AP01 link-encryption
```

AP Name	Encryption State	Dnstream Count	Upstream Count	Last 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to display TCP MSS for an access point:

```
Switch# 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	
<i>ap-name</i>	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:

```
Switch# 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:

```
Switch# 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 apnameap -namewlan dot1124ghzservice-policy
```

```
show apnameap -namewlan dot115ghzservice-policy
```

Syntax Description	
<i>ap- name</i>	Name of the Cisco lightweight access point.
<i>service-policy</i>	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.

```
Switch#show 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 switch, 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 switch 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:

```
Switch# 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 <i>ap-name</i>	(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:

```
Switch# 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 switch, 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 switch:

```
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	
<i>ap-name</i>	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 <i>token</i>	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:

```
Switch(config)# no trapflags ap register
```

wireless probe filter

To configure filtering of probe requests from AP, use **wireless probe filter** command. Use the **no** form of the command to disable the feature.

[no] wireless probe filter

Syntax Description	filter Configures filtering of probe requests from AP.				
Command Default	Enabled				
Command Modes	Global Configuration				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE Denali 16.3.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

Example

This example shows how to configure filtering of probe requests from AP.

```
Switch# wireless probe filter
```

wireless probe limit

To configure number of probe requests sent to the device per client per access point radio in a given interval, use **wireless probe limit** *num_probes interval* command. Use the **no** form of the command to disable the feature.

[no] wireless probe limit *num_probes interval*

Syntax Description	<i>num_probes</i>	Number of probe requests forwarded to the device per client per access point radio in a given interval. The range is from 1 to 100.
	<i>interval</i>	Probe limit interval in milliseconds. The range is from 100 to 10000
Command Default	None	
Command Modes	Global Configuration	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Example

This example shows how to configure 10 probe requests sent to the device per client per access point radio in an interval of 1000 milliseconds.

```
Switch# wireless probe limit 10 1000
```

wireless wps rogue ap rldp alarm-only

To configure an alarm when a rogue is detected, use **wirelesswps rogueaprl dp alarm-only** command. Use the **no** form of the command to disable the alarm.

[no] wireless wps rogue ap rldp alarm-only monitor-ap-only

Syntax Description	monitor-ap-only Perform RLDP only on monitor AP						
Command Default	None						
Command Modes	Global Configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> <tr> <td>Cisco IOS XE 3.7.3E</td> <td>The no form of the command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.	Cisco IOS XE 3.7.3E	The no form of the command was introduced.
Release	Modification						
Cisco IOS XE 3.2SE	This command was introduced.						
Cisco IOS XE 3.7.3E	The no form of the command was introduced.						

Example

This example shows how to configure an alarm for a detected rogue.

```
Switch#wireless wps rogue ap rldp alarm-only
```

wireless wps rogue ap rldp auto-contain

To configure RLDP, alarm and auto-contain if rogue is detected, use `wirelesswps rogueap rldp auto-contain` command. Use the **no** form of the command to disable the alarm.

[no] wireless wps rogue ap rldp auto-contain monitor-ap-only

Syntax Description	monitor-ap-only Perform RLDP only on monitor AP
Command Default	None
Command Modes	Global Configuration
Command History	Release Modification
	Cisco IOS XE 3.2SE This command was introduced.
	Cisco IOS XE 3.7.3E The no form of the command was introduced.

Example

This example shows how to configure an alarm for a detected rogue.

```
Switch#wireless wps rogue ap rldp auto-contain
```



PART VI

Mobility

- [Mobility Commands, on page 485](#)



Mobility Commands

- [mobility anchor](#), on page 486
- [wireless mobility](#), on page 488
- [wireless mobility controller](#), on page 489
- [wireless mobility controller \(ip_address\)](#) , on page 491
- [wireless mobility controller peer-group](#), on page 492
- [wireless mobility group keepalive](#), on page 493
- [wireless mobility group member ip](#), on page 494
- [wireless mobility group name](#) , on page 495
- [wireless mobility load-balance](#), on page 496
- [show wireless mobility](#), on page 497
- [clear wireless mobility statistics](#), on page 498

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 switch 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:

```
Switch(config-wlan)# mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Switch(config-wlan)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Switch(config-wlan)# mobility anchor
```

wireless mobility

To configure the interswitch mobility manager, use the **wireless mobility** command.

```
wireless mobility {dscp value }
```

Syntax Description	dscp value Configures the Mobility interswitch 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 shows how to configure mobility interswitch DSCP with an value of 20:

```
Switch(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 }}
no
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 }}
```

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 switch bridge domain ID.

```
Switch (config)# wireless mobility controller peer-group SPG1 bridge-domain-id 111
```

This example shows how to create and configure a switch peer group with a bridge ID of 111:

```
Switch(config)# controller peer-group TestDocPeerGroup bridge-domain-id 111
```

This example shows how to disable a switch peer group with a bridge ID of 111:

```
Switch(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):

```
Switch (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):

```
Switch (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 wireless mobility controller ip-address**

```
wireless mobility controller [ip ip-address [public-ip public-ip-address ]]
no wireless mobility controller
no wireless mobility controller ip ip-address
```

Syntax Description	<p>ip <i>ip-address</i> IP address of mobility controller.</p> <p>public-ip <i>public-ip-address</i></p>				
Command Default	None.				
Command Modes	Global Configuration.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>This command is valid only for the converged access switch.</p> <p>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.</p> <p>This examples shows how the controller communicates with the wireless management interface :</p> <pre>Switch (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6</pre> <p>This examples shows how to add a NAT option along with the wireless managed interface, when the target controller uses NAT:</p> <pre>Switch (config)# wireless mobility controller peer-group SPG1 member ip 10.10.20.6 public-ip 10.21.21.2</pre>				

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		
	<i>peer group</i>	Name of the peer group.
	member IP	Adds a peer group member.
	<i>ip-address</i>	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.

```
Switch enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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** *number*|**interval** *interval*}

Syntax Description	<p>count <i>number</i> 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.</p> <p>interval <i>interval</i> 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.</p>				
Command Default	3 seconds for count and 10 seconds for interval.				
Command Modes	Global Configuration.				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>The default values for <i>interval</i> is ten seconds and the default for <i>retries</i> is set to three.</p> <p>This example shows how to specify the amount of time between each ping request sent to a mobility group member to 10 seconds:</p> <pre>Switch(config)# wireless mobility group keepalive count 10</pre>				

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	<i>ip-address</i>	The IP address of the member controller.
	public-ip <i>public-ip-address</i>	(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 <i>group-name</i>	(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:

```
Switch(config)# mobility group member ip 10.104.171.101 group TestDocGroup
```

wireless mobility group name

To configure the 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:

```
Switch(config)# wireless 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 <i>threshold</i> 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	<ul style="list-style-type: none"> • 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.

```
Switch(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 <i>mobility-agent-ip</i> client summary		Shows the active clients on a mobility agent.
ap-list ip-address <i>ip-address</i>		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:

```
Switch (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:

```
Switch (config)# clear wireless mobility statistics
```



PART **VII**

Network Management

- [Network Management](#) , on page 501



Network Management

- [ip wccp](#), on page 503
- [monitor capture \(interface/control plane\)](#), on page 505
- [monitor capture buffer](#), on page 509
- [monitor capture clear](#), on page 510
- [monitor capture export](#), on page 511
- [monitor capture file](#), on page 512
- [monitor capture limit](#), on page 514
- [monitor capture match](#), on page 515
- [monitor capture start](#), on page 516
- [monitor capture stop](#), on page 517
- [monitor session](#), on page 518
- [monitor session destination](#), on page 520
- [monitor session filter](#), on page 524
- [monitor session source](#), on page 526
- [show ip sla statistics](#), on page 529
- [show monitor](#), on page 531
- [show monitor capture](#), on page 534
- [show platform ip wccp](#), on page 536
- [snmp-server enable traps](#), on page 537
- [snmp-server enable traps bridge](#), on page 540
- [snmp-server enable traps bulkstat](#), on page 541
- [snmp-server enable traps call-home](#), on page 542
- [snmp-server enable traps cef](#), on page 543
- [snmp-server enable traps cpu](#), on page 544
- [snmp-server enable traps envmon](#), on page 545
- [snmp-server enable traps errdisable](#), on page 546
- [snmp-server enable traps flash](#), on page 547
- [snmp-server enable traps isis](#), on page 548
- [snmp-server enable traps license](#), on page 549
- [snmp-server enable traps mac-notification](#), on page 550
- [snmp-server enable traps ospf](#), on page 551
- [snmp-server enable traps pim](#), on page 552
- [snmp-server enable traps port-security](#), on page 553

- [snmp-server enable traps power-ethernet](#), on page 554
- [snmp-server enable traps snmp](#), on page 555
- [snmp-server enable traps stackwise](#), on page 556
- [snmp-server enable traps storm-control](#), on page 558
- [snmp-server enable traps stpx](#), on page 559
- [snmp-server enable traps transceiver](#), on page 560
- [snmp-server enable traps vrfmib](#), on page 561
- [snmp-server enable traps vstack](#), on page 562
- [snmp-server engineID](#), on page 563
- [snmp-server host](#), on page 564
- [switchport mode access](#), on page 568
- [switchport voice vlan](#), on page 569

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 switch. 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).
<i>service-number</i>		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 <i>groupaddress</i>		(Optional) Specifies the multicast group address used by the switches and the application engines to participate in the service group.
group-list <i>access-list</i>		(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 <i>access-list</i>		(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.
password <i>encryption-number</i> <i>password</i>		(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 switch combines the password with the MD5 authentication value to create security for the connection between the switch 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 switch 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 switch 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:

```
Switch(config)# ip wccp web-cache
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 172.20.10.30 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport
Switch(config-if)#
*Dec 6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Switch(config-if)# ip address 175.20.20.10 255.255.255.0
Switch(config-if)# no shutdown
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# ip wccp web-cache group-listen
Switch(config-if)# exit
```

Related Topics

[show platform ip wccp](#), on page 536

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		
<i>capture-name</i>		The name of the capture to be defined.
interface <i>interface-type interface-id</i>		Specifies an interface with <i>interface-type</i> and <i>interface-id</i> as an attachment point. The arguments have these meanings: <ul style="list-style-type: none"> • GigabitEthernet <i>interface-id</i>—A Gigabit Ethernet IEEE 802.3z interface. • vlan <i>vlan-id</i>—A VLAN. The range for <i>vlan-id</i> is 1 to 4095. • capwap <i>capwap-id</i>—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. <p>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.</p>
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:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# 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:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in
Switch# monitor capture mycap match ipv4 any any
Switch# monitor capture mycap control-plane in
Switch# 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:

```
Switch# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet1/0/1 in
monitor capture mycap control-plane in
Switch# no monitor capture mycap control-plane
Switch# show monitor capture mycap parameter
monitor capture mycap interface GigabitEthernet1/0/1 in
```

To define a capture point with a CAPWAP attachment point:

```
Switch# 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

```
Switch# monitor capture mycap interface capwap 0 both
Switch# monitor capture mycap file location flash:mycap.pcap
Switch# monitor capture mycap file buffer-size 1
Switch# monitor capture mycap start
```

```
*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on
```

```
Switch# 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
Switch#
Switch# 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)
Switch#
Switch# 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=.....

```

Related Topics

- [monitor capture buffer](#), on page 509
- [monitor capture file](#), on page 512
- [show monitor capture](#), on page 534

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	<i>capture-name</i>	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 <i>buffer-size</i>	(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:

```
Switch# monitor capture mycap buffer circular size 1
```

Related Topics

- [monitor capture \(interface/control plane\)](#), on page 505
- [monitor capture file](#), on page 512
- [show monitor capture](#), on page 534

monitor capture clear

To clear the monitor capture (WireShark) buffer, use the **monitor capture clear** command in privileged EXEC mode.

monitor capture {*capture-name*} **clear**

Syntax Description	<i>capture-name</i> 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:

```
Switch# 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	<i>capture-name</i>	The name of the capture to be exported.
	<i>file-location</i> : <i>file-name</i>	(Optional) Specifies the location and file name of the capture storage file. Acceptable values for <i>file-location</i> : <ul style="list-style-type: none"> • 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:

```
Switch# 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		
<i>capture-name</i>		The name of the capture to be modified.
buffer-size <i>temp-buffer-size</i>		(Optional) Specifies the size of the temporary buffer. The range for <i>temp-buffer-size</i> is 1 to 100 MB. This is specified to reduce packet loss.
location <i>file-location</i> : <i>file-name</i>		(Optional) Specifies the location and file name of the capture storage file. Acceptable values for <i>file-location</i> : <ul style="list-style-type: none"> • flash—On-board flash storage • (usbflash0:)—USB drive
ring <i>number-of-ring-files</i>		(Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring.
size <i>total-size</i>		(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:

```
Switch# monitor capture mycap file location flash:mycap.pcap
```

Related Topics

[monitor capture \(interface/control plane\)](#), on page 505

[monitor capture buffer](#), on page 509

[show monitor capture](#), on page 534

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 <i>seconds</i>	(Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
packet-length <i>size</i>	(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 <i>num</i>	(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:

```
Switch# 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		
<i>capture-name</i>		The name of the capture to be assigned a core filter.
any		Specifies all packets.
mac <i>mac-match-string</i>		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:

```
Switch# monitor capture mycap interface GigabitEthernet1/0/1 in  
Switch# 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	<i>capture-name</i> 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:

```
Switch# 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	<i>capture-name</i> 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:

```
Switch# 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		
	<i>session-number</i>	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 <i>session-range</i>	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.

```
Switch(config)# monitor session 1 source interface Po13
Switch(config)# monitor session 1 filter vlan 1281
Switch(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
replicate
Switch(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:

```
Switch# 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
...
```

Related Topics

- [monitor session destination](#), on page 520
- [monitor session filter](#), on page 524
- [monitor session source](#), on page 526
- [show monitor](#), on page 531

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

<i>session-number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
interface <i>interface-id</i>	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 <i>vlan-id</i>	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:

```
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 delete a destination port from an existing local SPAN session:

```
Switch(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:

```
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(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.

```
Switch(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.

```
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```

Related Topics

- [monitor session](#), on page 518
- [monitor session filter](#), on page 524
- [monitor session source](#), on page 526
- [show monitor](#), on page 531

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		
<i>session-number</i>		The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
vlan <i>vlan-id</i>		Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <i>vlan-id</i> 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
```

Related Topics

- [monitor session](#), on page 518
- [monitor session destination](#), on page 520
- [monitor session source](#), on page 526
- [show monitor](#), on page 531

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		
<i>session_number</i>		The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
interface <i>interface-id</i>		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 <i>vlan-id</i>		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
```

Related Topics

[monitor session](#), on page 518

[monitor session destination](#), on page 520

[monitor session filter](#), on page 524

[show monitor](#), on page 531

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		
	<i>operation-number</i>	(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:

```
Switch# 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.
<i>session_number</i>		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 <i>list</i> 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:

```
Switch# 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:

```

Switch# 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:

```

Switch# 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 : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged

```

Related Topics

- [monitor session](#), on page 518
- [monitor session destination](#), on page 520
- [monitor session filter](#), on page 524

[monitor session source](#), on page 526

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	
<i>capture-name</i>	(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 <i>file-location</i> : <i>file-name</i>	(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 <i>display-filter-string</i>	Filters the display content according to the <i>display-filter-string</i> .

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:

```
Switch# 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)
```

Related Topics

[monitor capture \(interface/control plane\)](#), on page 505

[monitor capture buffer](#), on page 509

[monitor capture file](#), on page 512

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 <i>switch-number</i>	(Optional) Displays WCCP information only for specified <i>switch-number</i> .	

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 switch is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Switch# 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
```

Related Topics

[ip wccp](#), on page 503

snmp-server enable traps

To enable the switch 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 switch stack, this trap refers to the insertion or removal of a switch 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.*
stp	(Optional) Enables SNMP STP 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 switch. 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.

Examples

This example shows how to enable more than one type of SNMP trap:

```
Switch(config)# snmp-server enable traps cluster
Switch(config)# snmp-server enable traps config
Switch(config)# snmp-server enable traps vtp
```

Related Topics

- [snmp-server enable traps bridge](#), on page 540
- [snmp-server enable traps call-home](#), on page 542
- [snmp-server enable traps cpu](#), on page 544
- [snmp-server enable traps envmon](#), on page 545
- [snmp-server enable traps errdisable](#), on page 546
- [snmp-server enable traps flash](#), on page 547
- [snmp-server enable traps license](#), on page 549
- [snmp-server enable traps mac-notification](#), on page 550
- [snmp-server enable traps port-security](#), on page 553
- [snmp-server enable traps power-ethernet](#), on page 554
- [snmp-server enable traps snmp](#), on page 555
- [snmp-server enable traps stackwise](#), on page 556
- [snmp-server enable traps storm-control](#), on page 558
- [snmp-server enable traps stpx](#), on page 559
- [snmp-server enable traps transceiver](#), on page 560
- [snmp-server enable traps vstack](#), on page 562
- [snmp-server host](#), on page 564
- [snmp-server enable traps bulkstat](#), on page 541
- [snmp-server enable traps cef](#), on page 543
- [snmp-server enable traps isis](#), on page 548
- [snmp-server enable traps ospf](#), on page 551
- [snmp-server enable traps pim](#), on page 552
- [snmp-server enable traps vrfmib](#), on page 561

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.

Examples

This example shows how to send bridge new root traps to the NMS:

```
Switch(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.

Examples

This example shows how to generate data-collection-MIB collection traps:

```
Switch(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.

Examples

This example shows how to generate SNMP message-send-fail traps:

```
Switch(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.

Examples

This example shows how to generate SNMP CEF inconsistency traps:

```
Switch(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.

Examples

This example shows how to generate CPU threshold notifications:

```
Switch(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.

Examples

This example shows how to generate fan traps:

```
Switch(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 <i>number-of-notifications</i>	(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.

Examples

This example shows how to set the number SNMP notifications of error-disabling to 2:

```
Switch(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.

Examples

This example shows how to generate SNMP flash insertion notifications:

```
Switch(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	<p>errors (Optional) Enables IS-IS error traps.</p> <p>state-change (Optional) Enables IS-IS state change traps.</p>				
Command Default	The sending of IS-IS traps is disabled.				
Command Modes	Global configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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	<p>Informs are not supported in SNMPv1.</p> <p>To enable more than one type of trap, you must enter a separate snmp-server enable traps command for each trap type.</p>				
Examples	<p>This example shows how to generate IS-IS error traps:</p> <pre>Switch(config)# snmp-server enable traps isis errors</pre>				

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.

Examples

This example shows how to generate license deployment traps:

```
Switch(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.

Examples

This example shows how to generate SNMP MAC notification change traps:

```
Switch(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.
<i>rate-limit-time</i>	(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.
<i>max-number-of-traps</i>	(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.

Examples

This example shows how to enable LSA traps:

```
Switch(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

Inform traps 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.

Examples

This example shows how to enable invalid PIM message traps:

```
Switch(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 <i>value</i>	(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.

Examples

This example shows how to enable port-security traps at a rate of 200 per second:

```
Switch(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	police
	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.	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.

Examples

This example shows how to enable power-over-Ethernet traps for group 1:

```
Switch(config)# snmp-server enable traps power-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.

Examples

This example shows how to enable a warmstart SNMP trap:

```
Switch(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.

Examples

This example shows how to generate StackWise stack power GLS traps:

```
Switch(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 <i>number-of-minutes</i>	(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.

Examples

This example shows how to set the SNMP storm-control trap rate to 10 traps per minute:

```
Switch(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.

Examples

This example shows how to generate SNMP STPX MIB inconsistency update traps:

```
Switch(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

a (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

Inform 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.

Examples

This example shows how to set all SNMP transceiver traps:

```
Switch(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.

Examples

This example shows how to generate vrfmib trunk down traps:

```
Switch(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

Inform traps 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.

Examples

This example shows how to generate SNMP Smart Install client-added traps:

```
Switch(config)# snmp-server enable traps vstack addition
```


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 switch. 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

<i>host-addr</i>	Name or Internet address of the host (the targeted recipient).
vrf <i>vrf-instance</i>	(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).
<i>community-string</i>	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 switch 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 switch 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.

Examples

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:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(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:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host myhost.cisco.com by using the community string public:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Topics

[snmp-server enable traps](#)

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.

Examples

This example shows how to set a single-VLAN interface

```
Switch(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 <i>vlan_id</i> 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 Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Switch(config-template)# switchport voice vlan 20
```




PART **VIII**

QoS

- [QoS](#) , on page 573
- [Auto-QoS](#), on page 625



QoS

This chapter contains the following QoS commands:

- [auto qos](#), on page 574
- [class](#), on page 575
- [class-map](#), on page 578
- [match \(class-map configuration\)](#), on page 580
- [match non-client-nrt](#), on page 583
- [match wlan user-priority](#), on page 584
- [policy-map](#), on page 585
- [priority](#), on page 588
- [qos queue-softmax-multiplier](#), on page 590
- [queue-buffers ratio](#), on page 591
- [queue-limit](#), on page 592
- [service-policy \(Wired\)](#), on page 594
- [service-policy \(WLAN\)](#), on page 596
- [set](#), on page 597
- [show ap name service-policy](#), on page 604
- [show ap name dot11](#), on page 605
- [show class-map](#), on page 608
- [show wireless client calls](#), on page 609
- [show wireless client dot11](#), on page 610
- [show wireless client mac-address \(Call Control\)](#), on page 611
- [show wireless client mac-address \(TCLAS\)](#), on page 612
- [show wireless client voice diagnostics](#), on page 613
- [show policy-map](#), on page 614
- [show wlan](#), on page 619
- [trust device](#), on page 622

auto qos

To enable Auto QoS Wireless Policy, use the **auto qos** command. To remove Auto QoS Wireless Policy, use the **no** form of this command.

auto qos **enterprise** | **guest** | **voice**

Syntax Description	enterprise Enables AutoQos Wireless Enterprise Policy.						
	guest Enables AutoQos Wireless Guest Policy						
	voice Enables AutoQos Wireless Voice Policy						
Command Default	None						
Command Modes	WLAN Configuration						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.7.0</td> <td>This command was introduced.</td> </tr> <tr> <td>E</td> <td></td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.7.0	This command was introduced.	E	
Release	Modification						
Cisco IOS XE 3.7.0	This command was introduced.						
E							

This example shows how to enable AutoQos Wireless Enterprise Policy.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#auto qos enterprise
```

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 597
- **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.

Examples

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.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Switch(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:

```
Switch# configure terminal
Switch(config)# class-map cm-3
Switch(config-cmap)# match ip dscp 30
Switch(config-cmap)# exit

Switch(config)# class-map cm-4
Switch(config-cmap)# match ip dscp 40
Switch(config-cmap)# exit

Switch(config)# policy-map pm3
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit

Switch(config-pmap)# class cm-3
Switch(config-pmap-c)# set dscp 4
Switch(config-pmap-c)# exit

Switch(config-pmap)# class cm-4
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit

Switch# 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
```

Related Topics

[class-map](#), on page 578

[policy-map](#), on page 585

[show policy-map](#), on page 614

[set](#), on page 597

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-anytype}] class-map-name
no class-map [{match-anytype}] 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.
<i>class-map-name</i>	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).

Examples

This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Switch(config)# access-list 103 permit ip any any dscp 10
Switch(config)# class-map class1
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Switch(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

Related Topics

[policy-map](#), on page 585

[show policy-map](#), on page 614

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 <i>acl-name</i>		Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.
<i>acl-index</i>		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 <i>class-map-name</i>		Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.
cos <i>cos-value</i>		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 <i>dscp-value</i>		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 <i>dscp-list</i>		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 <i>ip-precedence-list</i>		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 <i>precedence-value1</i> ... <i>value4</i>		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 <i>qos-group-value</i>	Identifies a specific QoS group value as a match criterion. The range is 0 to 31.
vlan <i>vlan-id</i>	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 <i>class-map-name</i> , cos <i>cos-value</i> , qos-group <i>qos-group-value</i> , and vlan <i>vlan-id</i> 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.

Examples

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:

```
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
```

```
Switch(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:

```
Switch(config) # class-map class3
Switch(config-cmap) # match ip precedence 5 6 7
Switch(config-cmap) # exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Switch(config) # class-map class2
Switch(config-cmap) # match ip precedence 5 6 7
Switch(config-cmap) # no match ip precedence
Switch(config-cmap) # match access-group acl1
Switch(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:

```
Switch(config) # class-map match-any class4
Switch(config-cmap) # match cos 4
Switch(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:

```
Switch(config) # class-map match-any class4
Switch(config-cmap) # match cos 4
Switch(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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	None				

This example show how you can configure non-client NRT:

```
Switch(config)# class-map test_1000
Switch(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	<i>wlan-value</i> 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 configuration (config-cmap)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	None				

This example show how you can configure user-priority values:

```
Switch(config)# class-map test_1000
Switch(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 (config)

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 switch.

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.

Examples

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.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# police 1000000 20000 conform-action transmit
Switch(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Switch# configure terminal
Switch(config)# class-map c1
Switch(config-cmap)# exit
```

```
Switch(config)# class-map c2
Switch(config-cmap)# exit
```

```
Switch(config)# policy-map child
Switch(config-pmap)# class c1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Switch(config-pmap-c-police)# exit
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class c2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
Switch(config)# policy-map parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 1000000
Switch(config-pmap-c)# service-policy child
Switchconfig-pmap-c)# end
```

This example shows how to delete a policy map:

```
Switch(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

[class](#), on page 575

[class-map](#), on page 578

[service-policy \(Wired\)](#), on page 594

[show policy-map](#), on page 614

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		
	<i>Kb/s</i>	(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.
	<i>burst -in-bytes</i>	(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 <i>level-value</i>	(Optional) Assigns priority level. Available values for <i>level-value</i> 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.
	percent <i>percentage</i>	(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 (config-pmap-c)

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE 3.3SE	The <i>Kbps</i> , <i>burst -in-bytes</i> , and percent percentage keywords were added.

Usage Guidelines 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.

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:

```
Switch(config)# class-map cm1
Switch(config-cmap)#match precedence 2
Switch(config-cmap)#exit

Switch(config)#class-map cm2
Switch(config-cmap)#match dscp 30
Switch(config-cmap)#exit

Switch(config)# policy-map policy1
Switch(config-pmap)# class cm1
Switch(config-pmap-c)# priority level 1
Switch(config-pmap-c)# police 1m
Switch(config-pmap-c-police)#exit
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit

Switch(config)#policy-map policy1
Switch(config-pmap)#class cm2
Switch(config-pmap-c)#priority level 2
Switch(config-pmap-c)#police 1m
```

qos queue-softmax-multiplier

To increase the value of softmax buffer, use the **qos queue-softmax-multiplier** command in the global configuration mode.

range-of-multiplier

no qos queue-softmax-multiplier *range-of-multiplier*

Syntax Description	<i>range-of-multiplier</i>	You can specify a value in the range of 100 to 1200. The default value is 100.
---------------------------	----------------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE 3.6.3 and Cisco IOS XE 3.7.2	This command was introduced.

Usage Guidelines



Note	This command would take effect only on the ports where a policy-map is attached. If configured as 1200, the softmax for non-priority queues and non-primary priority queue (!=level 1) are multiplied by 12 with their default values. This command is not applicable for priority queue level 1.
-------------	---

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	<i>ratio limit</i> (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 (config-pmap-c)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>Either the bandwidth, shape, or priority command must be used before using this command. For more information about these commands, see <i>Cisco IOS Quality of Service Solutions Command Reference</i> available on Cisco.com</p> <p>The switch 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.</p>				

Example

The following example sets the queue buffers ratio to 10 percent:

```
Switch(config)# policy-map policy_queuebuf01
Switch(config-pmap)# class-map class_queuebuf01
Switch(config-cmap)# exit
Switch(config)# policy policy_queuebuf01
Switch(config-pmap)# class class_queuebuf01
Switch(config-pmap-c)# bandwidth percent 80
Switch(config-pmap-c)# queue-buffers ratio 10
Switch(config-pmap)# end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

[show policy-map](#), on page 614

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

<i>queue-limit-size</i>	The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
cos <i>cos-value</i>	Specifies parameters for each cos value. CoS values are from 0 to 7.
dscp <i>dscp-value</i>	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 <i>percentage-of-packets</i>	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 (policy-map-c)

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:

```
Switch(config)# policy-map policy11
Switch(config-pmap)# class dscp-1
Switch(config-pmap-c)# bandwidth percent 20
Switch(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.

Examples

This example shows how to apply plcmap1 to an physical ingress port:

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(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:

```
Switch# configure terminal
```

```
Switch(config)# class-map vlan100
Switch(config-cmap)# match vlan 100
Switch(config-cmap)# exit
Switch(config)# policy-map vlan100
Switch(config-pmap)# policy-map class vlan100
Switch(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Switch(config-pmap-c-police)# end
Switch# configure terminal
Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# service-policy input vlan100
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Topics

[policy-map](#), on page 585

[show policy-map](#), on page 614

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.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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):

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

Related Topics

[wlan](#), on page 1207

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 <i>table-map-name</i> , 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.

Examples

This example shows how to assign DSCP 10 to all FTP traffic without any policers:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class-map ftp_class
Switch(config-cmap)# exit
Switch(config)# policy policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

Related Topics

- [class](#), on page 575
- [policy-map](#), on page 585
- [show policy-map](#), on page 614

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	<i>ap-name</i> Name of the Cisco lightweight access point.				
Command Default	None				
Command Modes	Any command mode				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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-policy output|stats|tsm
{allclient-mac}}
```

Syntax	Description
<i>ap-name</i>	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.
<i>client-mac</i>	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:

```
Switch# 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:

```
Switch# show ap name AP01 dot11 24ghz ccx
```

This example show how to display CDP information for a specific access point:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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 insufficient 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:

```
Switch# 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	
<i>class-map-name</i>	(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.

Examples

This is an example of output from the **show class-map** command:

```
Switch# 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
```

Related Topics

[class-map](#), on page 578

show wireless client calls

To display the total number of active or rejected calls on the switch, 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:

```
switch# 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:

```
Switch# 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	<i>mac-address</i>	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:

```
Switch# 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-3b3b0.3d27dale-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:

```
Switch# 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** | **rss** | **status** | **tspec**}

Syntax Description	Parameter	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.
	rss	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:

```
Switch# 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
<i>policy-map-name</i>	(Optional) Name of the policy-map.
interface <i>interface-id</i>	(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 <i>ap_name</i>	Displays SSID policy configuration of an access point.
client mac <i>mac_address</i>	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 <i>ssid_name</i>	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 <i>interface-id</i> 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.

To display classification counters for ternary content addressable memory (TCAM) (marking or policing) based policies, enter the interface ID. Classification counters have the following restrictions:

- Filter- based classification counters are not supported.
- Classification counters are supported only on wired ports (in the ingress and egress directions).
- Classification counters count packets instead of bytes.
- Only QoS configurations with marking or policing trigger the classification counter.
- As long as there is policing or marking action in the policy, the class-default will have classification counters.
- Classification counters are not port based. The counters are shared across targets sharing the same policy map. This means that the classification counter aggregates all packets belonging to the same class of the same policy which attach to different interfaces.

This is an example of output from the **show policy-map interface** command, where classification counters are displayed:

```
Switch# show policy-map interface gigabitethernet1/0/1

GigabitEthernet1/0/1

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
    cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 3
        0 packets, 0 bytes
        5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
```

```

conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes

```

```
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
```

```
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

Related Topics

[policy-map](#), on page 585

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 <i>wlan-id</i>		Specifies the wireless LAN identifier. The range is from 1 to 512.
name <i>wlan-name</i>		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:

```
Switch# 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:

```
Switch# 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:

```
Switch(config)# interface GigabitEthernet1/0/1  
Switch(config-if)# trust device cisco-phone
```

You can verify your settings by entering the **show interface status** privileged EXEC command.



Auto-QoS

This chapter contains the following auto-QoS commands:

- [auto qos classify](#), on page 626
- [auto qos trust](#), on page 632
- [auto qos video](#), on page 640
- [auto qos voip](#) , on page 651
- [debug auto qos](#), on page 664
- [show auto qos](#) , on page 665

auto qos classify

To automatically configure quality of service (QoS) classification for untrusted devices within a QoS domain, use the **auto qos classify** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

auto qos classify [police]
no auto qos classify [police]

Syntax Description

police (Optional) Configure QoS policing for untrusted devices.

Command Default

Auto-QoS classify is disabled on the port.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 18: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Auto-QoS configures the switch for connectivity with a trusted interface. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packets is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.



Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos classify** and **auto qos classify police** commands:

Policy maps (For the **auto qos classify police** command):

- AutoQos-4.0-Classify-Police-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos classify** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos classify** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS classification of an untrusted device and police traffic:

```
Switch(config)# interface gigabitEthernet1/0/6
Switch(config-if)# auto qos classify police
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/6

GigabitEthernet1/0/6

Service-policy input: AutoQos-4.0-Classify-Police-Input-Policy

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
    cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af21
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps
```

```
Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavanger
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs1
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Signaling
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
```

```

    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 750000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps

```

```
Match: cos 1
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
Match: dscp cs1 (8)
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

auto qos trust

To automatically configure quality of service (QoS) for trusted interfaces within a QoS domain, use the **auto qos trust** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
auto qos trust {cos|dscp}
no auto qos trust {cos|dscp}
```

Syntax Description

cos Trusts the CoS packet classification.

dscp Trusts the DSCP packet classification.

Command Default

Auto-QoS trust is disabled on the port.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to configure the QoS for trusted interfaces within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS. When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Table 19: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ⁵ BPDU ⁶ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ⁷	46	24, 26	48	56	34	–	
CoS ⁸	5	3	6	7	3	–	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)			0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

⁵ STP = Spanning Tree Protocol

⁶ BPDU = bridge protocol data unit

⁷ DSCP = Differentiated Services Code Point

⁸ CoS = class of service

Table 20: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	Up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6,7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent



Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos trust cos** command.

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)

- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos trust dscp** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos trust** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos trust** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Examples

This example shows how to enable auto-QoS for a trusted interface with specific CoS classification.

```
Switch(config)# interface gigabitEthernet1/0/17
Switch(config-if)# auto qos trust cos
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/17

GigabitEthernet1/0/17

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
```

```
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
```

```

    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 25%
    queue-buffers ratio 25

```

This example shows how to enable auto-QoS for a trusted interface with specific DSCP classification.

```

Switch(config)# interface GigabitEthernet1/0/18
Switch(config-if)# auto qos trust dscp
Switch(config-if)# end
Switch#show policy-map interface GigabitEthernet1/0/18

```

```
GigabitEthernet1/0/18

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
```

```

    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 4%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 1%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

```

```
(total drops) 0  
(bytes output) 0  
bandwidth remaining 25%  
queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

auto qos video

To automatically configure quality of service (QoS) for video within a QoS domain, use the **auto qos video** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

```
auto qos video {cts | ip-camera | media-player}
no auto qos video {cts | ip-camera | media-player}
```

Syntax Description

cts	Specifies a port connected to a Cisco TelePresence System and automatically configures QoS for video.
ip-camera	Specifies a port connected to a Cisco IP camera and automatically configures QoS for video.
media-player	Specifies a port connected to a CDP-capable Cisco digital media player and automatically configures QoS for video.

Command Default

Auto-QoS video is disabled on the port.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use this command to configure the QoS appropriate for video traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS. When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues. For more information, see the queue tables at the end of this section.

Auto-QoS configures the switch for video connectivity to a Cisco TelePresence system, a Cisco IP camera, or a Cisco digital media player.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.

The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos video cts** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video ip-camera** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos video media-player** command:

Policy maps:

- AutoQos-4.0-Trust-Dscp-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

To disable auto-QoS on a port, use the **no auto qos video** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled, and you enter the **no auto qos video** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

Table 21: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ⁹ BPDUs ¹⁰ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ¹¹	46	24, 26	48	56	34	—	
CoS ¹²	5	3	6	7	3	—	
CoS-to-egress queue map	4, 5 (queue 1)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	2, 3, 6, 7 (queue 2)	0 (queue 3)	2 (queue 3)	0, 1 (queue 4)

⁹ STP = Spanning Tree Protocol

¹⁰ BPDUs = bridge protocol data unit

¹¹ DSCP = Differentiated Services Code Point

¹² CoS = class of service

Table 22: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	up to 100 percent	25 percent	15 percent

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Examples

The following is an example of the **auto qos video cts** command and the applied policies and class maps:

```
Switch(config)# interface gigabitEthernet1/0/12
Switch(config-if)# auto qos video cts
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/12

GigabitEthernet1/0/12

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

    queue stats for all priority classes:
      Queueing
        priority level 1

        (total drops) 0
        (bytes output) 0

    Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
      0 packets
      Match: dscp cs4 (32) cs5 (40) ef (46)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 5
        0 packets, 0 bytes
        5 minute rate 0 bps
      Priority: 30% (300000 kbps), burst bytes 7500000,
      Priority Level: 1

    Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
      0 packets
      Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: cos 3
        0 packets, 0 bytes
        5 minute rate 0 bps
      Queueing
```

```

queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0

```

```

(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

The following is an example of the **auto qos video ip-camera** command and the applied policies and class maps:

```

Switch(config)# interface GigabitEthernet1/0/9
Switch(config-if)# auto qos video ip-camera
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/9

GigabitEthernet1/0/9

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
QoS Set
 dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
Queueing
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes

```

```

    5 minute rate 0 bps
Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 1

```

```

    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
   0 packets, 0 bytes
   5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
   0 packets, 0 bytes
   5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
   0 packets, 0 bytes
   5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

The following is an example of the **auto qos video media-player** command and the applied policies and class maps.

```

Switch(config)# interface GigabitEthernet1/0/7
Switch(config-if)# auto qos video media-player
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/7

GigabitEthernet1/0/7

Service-policy input: AutoQos-4.0-Trust-Dscp-Input-Policy

Class-map: class-default (match-any)
 0 packets
Match: any
   0 packets, 0 bytes

```

```

    5 minute rate 0 bps
  QoS Set
    dscp dscp table AutoQos-4.0-Trust-Dscp-Table

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: 30% (300000 kbps), burst bytes 7500000,

  Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
  queue-limit dscp 16 percent 80
  queue-limit dscp 24 percent 90
  queue-limit dscp 48 percent 100
  queue-limit dscp 56 percent 100

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%

  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes

```

```
    5 minute rate 0 bps
Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos video interface *interface-id*** privileged EXEC command.

auto qos voip

To automatically configure quality of service (QoS) for voice over IP (VoIP) within a QoS domain, use the **auto qos voip** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

```
auto qos voip {cisco-phone | cisco-softphone | trust}
no auto qos voip {cisco-phone | cisco-softphone | trust}
```

Syntax Description	
cisco-phone	Specifies a port connected to a Cisco IP phone, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted only when the telephone is detected.
cisco-softphone	Specifies a port connected to a device running the Cisco SoftPhone, and automatically configures QoS for VoIP.
trust	Specifies a port connected to a trusted switch, and automatically configures QoS for VoIP. The QoS labels of incoming packets are trusted. For nonrouted ports, the CoS value of the incoming packet is trusted. For routed ports, the DSCP value of the incoming packet is trusted.

Command Default Auto-QoS is disabled on the port.

When auto-QoS is enabled, it uses the ingress packet label to categorize traffic, to assign packet labels, and to configure the ingress and egress queues.

Command Default Interface configuration

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

Usage Guidelines Use this command to configure the QoS appropriate for VoIP traffic within the QoS domain. The QoS domain includes the switch, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the switch for VoIP with Cisco IP phones on switch and routed ports and for devices running the Cisco SoftPhone application. These releases support only Cisco IP SoftPhone Version 1.3(3) or later. Connected devices must use Cisco Call Manager Version 4 or later.

To take advantage of the auto-QoS defaults, you should enable auto-QoS before you configure other QoS commands. You can fine-tune the auto-QoS configuration *after* you enable auto-QoS.



Note The switch applies the auto-QoS-generated commands as if the commands were entered from the command-line interface (CLI). An existing user configuration can cause the application of the generated commands to fail or to be overridden by the generated commands. These actions occur without warning. If all the generated commands are successfully applied, any user-entered configuration that was not overridden remains in the running configuration. Any user-entered configuration that was overridden can be retrieved by reloading the switch without saving the current configuration to memory. If the generated commands fail to be applied, the previous running configuration is restored.

If this is the first port on which you have enabled auto-QoS, the auto-QoS-generated global configuration commands are executed followed by the interface configuration commands. If you enable auto-QoS on another port, only the auto-QoS-generated interface configuration commands for that port are executed.

When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of the network that is connected to a Cisco IP phone, the switch enables the trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the port is set to trust the QoS label received in the packet. The switch also uses policing to determine whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The policing is applied to those traffic matching the policy-map classification before the switch enables the trust boundary feature.

-
- When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0.
- When you enter the **auto qos voip trust** interface configuration command on a port connected to the network interior, the switch trusts the CoS value for nonrouted ports or the DSCP value for routed ports in ingress packets (the assumption is that traffic has already been classified by other edge devices).

You can enable auto-QoS on static, dynamic-access, and voice VLAN access, and trunk ports. When enabling auto-QoS with a Cisco IP phone on a routed port, you must assign a static IP address to the IP phone.



Note

When a device running Cisco SoftPhone is connected to a switch or routed port, the switch supports only one Cisco SoftPhone application per port.

After auto-QoS is enabled, do not modify a policy map or aggregate policer that includes *AutoQoS* in its name. If you need to modify the policy map or aggregate policer, make a copy of it, and change the copied policy map or policer. To use the new policy map instead of the generated one, remove the generated policy map from the interface, and apply the new policy map.

To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. Use the **debug auto qos** privileged EXEC command to enable auto-QoS debugging.

The following policy maps and class maps are created and applied when running the **auto qos voip trust** command:

Policy maps:

- AutoQos-4.0-Trust-Cos-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)

- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-softphone** command:

Policy maps:

- AutoQos-4.0-CiscoSoftPhone-Input-Policy
- AutoQos-4.0-Output-Policy

Class maps:

- AutoQos-4.0-Voip-Data-Class (match-any)
- AutoQos-4.0-Voip-Signal-Class (match-any)
- AutoQos-4.0-Multimedia-Conf-Class (match-any)
- AutoQos-4.0-Bulk-Data-Class (match-any)
- AutoQos-4.0-Transaction-Class (match-any)
- AutoQos-4.0-Scavenger-Class (match-any)
- AutoQos-4.0-Signaling-Class (match-any)
- AutoQos-4.0-Default-Class (match-any)
- class-default (match-any)
- AutoQos-4.0-Output-Priority-Queue (match-any)
- AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
- AutoQos-4.0-Output-Trans-Data-Queue (match-any)
- AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
- AutoQos-4.0-Output-Scavenger-Queue (match-any)
- AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)

The following policy maps and class maps are created and applied when running the **auto qos voip cisco-phone** command:

Policy maps:

- service-policy input AutoQos-4.0-CiscoPhone-Input-Policy

- service-policy output AutoQos-4.0-Output-Policy

Class maps:

- class AutoQos-4.0-Voip-Data-CiscoPhone-Class
- class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
- class AutoQos-4.0-Default-Class

To disable auto-QoS on a port, use the **no auto qos voip** interface configuration command. Only the auto-QoS-generated interface configuration commands for this port are removed. If this is the last port on which auto-QoS is enabled and you enter the **no auto qos voip** command, auto-QoS is considered disabled even though the auto-QoS-generated global configuration commands remain (to avoid disrupting traffic on other ports affected by the global configuration).

The switch configures egress queues on the port according to the settings in this table.

Table 23: Auto-QoS Configuration for the Egress Queues

Egress Queue	Queue Number	CoS-to-Queue Map	Queue Weight (Bandwidth)	Queue (Buffer) Size for Gigabit-Capable Ports	Queue (Buffer) Size for 10/100 Ethernet Ports
Priority (shaped)	1	4, 5	Up to 100 percent	25 percent	15 percent
SRR shared	2	2, 3, 6, 7	10 percent	25 percent	25 percent
SRR shared	3	0	60 percent	25 percent	40 percent
SRR shared	4	1	20 percent	25 percent	20 percent

Examples

The following is an example of the **auto qos voip trust** command and the applied policies and class maps:

```
Switch(config)# interface gigabitEthernet1/0/31
Switch(config-if)# auto qos voip trust
Switch(config-if)# end
Switch# show policy-map interface GigabitEthernet1/0/31

GigabitEthernet1/0/31

  Service-policy input: AutoQos-4.0-Trust-Cos-Input-Policy

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
      QoS Set
        cos cos table AutoQos-4.0-Trust-Cos-Table

  Service-policy output: AutoQos-4.0-Output-Policy

  queue stats for all priority classes:
    Queueing
```

```
priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
```

```

bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
 0 packets
Match: dscp af11 (10) af12 (12) af13 (14)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 1
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

The following is an example of the **auto qos voip cisco-phone** command and the applied policies and class maps:

```

Switch(config)# interface gigabitEthernet1/0/5
Switch(config-if)# auto qos voip cisco-phone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/5

```

GigabitEthernet1/0/5

Service-policy input: AutoQos-4.0-CiscoPhone-Input-Policy

```
Class-map: AutoQos-4.0-Voip-Data-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 5
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp ef
  police:
    cir 128000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps
```

```
Class-map: AutoQos-4.0-Voip-Signal-CiscoPhone-Class (match-any)
  0 packets
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps
```

```
Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Default
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp default
```

```
Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
```

Service-policy output: AutoQos-4.0-Output-Policy

```
queue stats for all priority classes:
  Queueing
  priority level 1

  (total drops) 0
  (bytes output) 0
```

```
Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
  0 packets
  Match: dscp cs4 (32) cs5 (40) ef (46)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 5
    0 packets, 0 bytes
```

```

    5 minute rate 0 bps
    Priority: 30% (300000 kbps), burst bytes 7500000,

    Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
  0 packets
  Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing
    queue-limit dscp 16 percent 80
    queue-limit dscp 24 percent 90
    queue-limit dscp 48 percent 100
    queue-limit dscp 56 percent 100

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%

    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
  0 packets
  Match: dscp af41 (34) af42 (36) af43 (38)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 4
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
  0 packets
  Match: dscp af21 (18) af22 (20) af23 (22)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 2
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

    (total drops) 0
    (bytes output) 0
    bandwidth remaining 10%
    queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

```

```

(total drops) 0
(bytes output) 0
bandwidth remaining 4%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
 0 packets
Match: dscp cs1 (8)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 1%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
 0 packets
Match: dscp af31 (26) af32 (28) af33 (30)
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: class-default (match-any)
 0 packets
Match: any
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 25%
queue-buffers ratio 25

```

The following is an example of the **auto qos voip cisco-softphone** command and the applied policies and class maps:

```

Switch(config)# interface gigabitEthernet1/0/20
Switch(config-if)# auto qos voip cisco-softphone
Switch(config-if)# end
Switch# show policy-map interface gigabitEthernet1/0/20

GigabitEthernet1/0/20

Service-policy input: AutoQos-4.0-CiscoSoftPhone-Input-Policy

Class-map: AutoQos-4.0-Voip-Data-Class (match-any)
 0 packets
Match: dscp ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps

```

```

QoS Set
  dscp ef
police:
  cir 128000 bps, bc 8000 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    set-dscp-transmit dscp table policed-dscp
  conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Voip-Signal-Class (match-any)
  0 packets
  Match: dscp cs3 (24)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 3
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Multimedia-Conf-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af41
  police:
    cir 5000000 bps, bc 156250 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Bulk-Data-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Bulk-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set
    dscp af11
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Transaction-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Transactional-Data
    0 packets, 0 bytes
    5 minute rate 0 bps
  QoS Set

```

```

    dscp af21
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Scavanger-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Scavanger
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp cs1
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Signaling-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Signaling
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp cs3
  police:
    cir 32000 bps, bc 8000 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop
    conformed 0000 bps, exceed 0000 bps

Class-map: AutoQos-4.0-Default-Class (match-any)
  0 packets
Match: access-group name AutoQos-4.0-Acl-Default
  0 packets, 0 bytes
  5 minute rate 0 bps
QoS Set
  dscp default
  police:
    cir 10000000 bps, bc 312500 bytes
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      set-dscp-transmit dscp table policed-dscp
    conformed 0000 bps, exceed 0000 bps

Class-map: class-default (match-any)
  0 packets
Match: any
  0 packets, 0 bytes
  5 minute rate 0 bps

Service-policy output: AutoQos-4.0-Output-Policy

queue stats for all priority classes:
  Queueing

```

```

priority level 1

(total drops) 0
(bytes output) 0

Class-map: AutoQos-4.0-Output-Priority-Queue (match-any)
 0 packets
Match: dscp cs4 (32) cs5 (40) ef (46)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 5
 0 packets, 0 bytes
 5 minute rate 0 bps
Priority: 30% (300000 kbps), burst bytes 7500000,

Priority Level: 1

Class-map: AutoQos-4.0-Output-Control-Mgmt-Queue (match-any)
 0 packets
Match: dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 3
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing
queue-limit dscp 16 percent 80
queue-limit dscp 24 percent 90
queue-limit dscp 48 percent 100
queue-limit dscp 56 percent 100

(total drops) 0
(bytes output) 0
bandwidth remaining 10%

queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Conf-Queue (match-any)
 0 packets
Match: dscp af41 (34) af42 (36) af43 (38)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 4
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Trans-Data-Queue (match-any)
 0 packets
Match: dscp af21 (18) af22 (20) af23 (22)
 0 packets, 0 bytes
 5 minute rate 0 bps
Match: cos 2
 0 packets, 0 bytes
 5 minute rate 0 bps
Queueing

(total drops) 0
(bytes output) 0

```

```
bandwidth remaining 10%
queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Bulk-Data-Queue (match-any)
  0 packets
  Match: dscp af11 (10) af12 (12) af13 (14)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Match: cos 1
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 4%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Scavenger-Queue (match-any)
  0 packets
  Match: dscp cs1 (8)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 1%
  queue-buffers ratio 10

Class-map: AutoQos-4.0-Output-Multimedia-Strm-Queue (match-any)
  0 packets
  Match: dscp af31 (26) af32 (28) af33 (30)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

Class-map: class-default (match-any)
  0 packets
  Match: any
    0 packets, 0 bytes
    5 minute rate 0 bps
  Queueing

  (total drops) 0
  (bytes output) 0
  bandwidth remaining 25%
  queue-buffers ratio 25
```

You can verify your settings by entering the **show auto qos interface *interface-id*** privileged EXEC command.

debug auto qos

To enable debugging of the automatic quality of service (auto-QoS) feature, use the **debug auto qos** command in privileged EXEC mode. Use the **no** form of this command to disable debugging.

debug auto qos
no debug auto qos

Syntax Description This command has no arguments or keywords.

Command Default Auto-QoS debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines To display the QoS configuration that is automatically generated when auto-QoS is enabled, enable debugging before you enable auto-QoS. You enable debugging by entering the **debug auto qos** privileged EXEC command.

The **undebug auto qos** command is the same as the **no debug auto qos** 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** privileged EXEC command. Then enter the **debug** command at the command-line prompt of the stack member. You also can use the **remote command stack-member-number LINE** privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Switch# debug auto qos
AutoQoS debugging is on
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# auto qos voip cisco-phone
```

show auto qos

To display the quality of service (QoS) commands entered on the interfaces on which automatic QoS (auto-QoS) is enabled, use the **show auto qos** command in privileged EXEC mode.

```
show auto qos [interface [interface-id]]
```

Syntax Description	interface [<i>interface-id</i>]	(Optional) Displays auto-QoS information for the specified port or for all ports. Valid interfaces include physical ports.
---------------------------	---	--

Command Modes	User EXEC Privileged EXEC
----------------------	------------------------------

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

Usage Guidelines

The **show auto qos** command output shows only the **auto qos** command entered on each interface. The **show auto qos interface interface-id** command output shows the **auto qos** command entered on a specific interface. Use the **show running-config** privileged EXEC command to display the auto-QoS configuration and the user modifications.

Beginning in Cisco IOS Release 12.2(40)SE, the **show auto qos** command output shows the service policy information for the Cisco IP phone.

Examples

This is an example of output from the **show auto qos** command after the **auto qos voip cisco-phone** and the **auto qos voip cisco-softphone** interface configuration commands are entered:

```
Switch# show auto qos
GigabitEthernet2/0/4
auto qos voip cisco-softphone

GigabitEthernet2/0/5
auto qos voip cisco-phone

GigabitEthernet2/0/6
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface interface-id** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet 2/0/5
GigabitEthernet2/0/5
auto qos voip cisco-phone
```

This is an example of output from the **show auto qos interface interface-id** command when the **auto qos voip cisco-phone** interface configuration command is entered:

```
Switch# show auto qos interface gigabitethernet1/0/2
GigabitEthernet1/0/2
auto qos voip cisco-phone
```

These are examples of output from the **show auto qos interface *interface-id*** command when auto-QoS is disabled on an interface:

```
Switch# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```



PART **IX**

Radio Resource Management

- [Radio Resource Management Commands, on page 669](#)



Radio Resource Management Commands

- [airtime-fairness dot11 mode \(apgroup\)](#), on page 671
- [airtime-fairness dot11 optimization \(apgroup\)](#), on page 672
- [airtime-fairness dot11 policy](#), on page 673
- [airtime-fairness policy \(wlan\)](#), on page 674
- [ap dot11 rf-profile](#), on page 675
- [ap dot11 rrm](#), on page 676
- [ap dot11 rrm ccx](#), on page 679
- [ap dot11 rrm channel](#), on page 680
- [ap dot11 24ghz rrm channel cleanair-event rogue-contribution](#), on page 681
- [ap dot11 24ghz or 5ghz rrm channel dca add](#), on page 682
- [ap dot11 24ghz or 5ghz rrm channel dca remove](#), on page 683
- [ap dot11 5ghz rrm channel dca chan-width width-max](#), on page 684
- [ap dot11 rrm coverage](#), on page 685
- [ap dot11 rrm group-member](#), on page 687
- [ap dot11 rrm monitor](#), on page 688
- [ap dot11 rrm profile](#), on page 689
- [ap dot11 rrm tpc-threshold](#), on page 690
- [ap dot11 rrm txpower](#), on page 691
- [ap dot11 airtime-fairness mode](#), on page 692
- [ap dot11 airtime-fairness policy-name](#), on page 693
- [ap group](#), on page 695
- [ap name dot11 airtime-fairness mode](#), on page 696
- [ap name dot11 airtime-fairness optimization](#), on page 697
- [ap name no dot11 airtime-fairness wlan-name policy-name](#), on page 698
- [ap name dot11 airtime-fairness wlan-name policy](#), on page 699
- [band-select client](#), on page 700
- [band-select cycle](#), on page 701
- [band-select expire](#), on page 702
- [band-select probe-response](#), on page 703
- [channel](#), on page 704
- [channel foreign](#), on page 705
- [channel width](#), on page 706
- [coverage](#), on page 707

- coverage exception, on page 708
- coverage level, on page 709
- clear wireless airtime-fairness statistics, on page 710
- dot11n-only, on page 711
- load-balancing, on page 712
- high-density clients count, on page 713
- high-density clients wlan, on page 714
- high-density multicast data-rate, on page 715
- high-density rx-sop threshold, on page 716
- rate, on page 717
- rate mcs, on page 718
- trap threshold, on page 719
- tx-power, on page 720
- tx-power v1 threshold, on page 721
- no ap dot11 airtime-fairness policy-name, on page 722
- remote-lan, on page 723
- rf-profile dot11 24ghz, on page 724
- rf-profile dot11 5ghz, on page 725
- show ap airtime-fairness ap-group, on page 726
- show ap airtime-fairness (ap), on page 727
- show ap airtime-fairness (per radio), on page 728
- show ap airtime-fairness policy (all), on page 729
- show ap airtime-fairness wlan, on page 730
- show ap dot11 24ghz , on page 731
- show ap dot11 5ghz, on page 733
- show ap dot11 airtime-fairness (radio bands), on page 735
- show ap dot11 24ghz rf-profile summary, on page 736
- show ap dot11 5ghz rf-profile summary, on page 737
- show ap name dot11 airtime-fairness summary, on page 738
- show ap name dot11 airtime-fairness policy statistics, on page 739
- show ap name dot11 airtime-fairness wlan name statistics, on page 740
- show ap rf-profile summary, on page 741
- show ap rf-profile name, on page 742
- show wireless mobility controller ap, on page 744
- shutdown, on page 745
- wlan, on page 746

airtime-fairness dot11 mode (apgroup)

To configure ATF for an AP group, use the **airtime-fairness dot11 mode** command in ap group submode. Use the **no** form of the command to disable ATF for a AP group.

```
airtime-fairness dot11 {24ghz|5ghz} mode {enforce-policy|monitor}
```

```
no airtime-fairness dot11 {24ghz|5ghz} mode {enforce-policy|monitor}
```

Syntax	Description
24ghz	Configures 802.11b parameters
5ghz	Configures 802.11a parameters
enforce-policy	Configure airtime-fairness in enforce-policy mode
monitor	Configure airtime-fairness in monitor mode

Command Default None

Command Modes config apgroup

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines None

This example shows how to configure ATF for an AP group.

```
Switch#configure terminal
Switchconfig# ap group testap
Switchconfig-apgroup# airtime-fairness dot11 24ghz mode monitor
```

airtime-fairness dot11 optimization (apgroup)

To configure ATF optimization for an AP group, use the **airtime-fairness dot11 optimization** command. Use the **no** form of the command to disable ATF for a AP group

airtime-fairness dot11 {24ghz|5ghz} optimization

no airtime-fairness dot11 {24ghz|5ghz} optimization

Syntax Description	24ghz	Configures 802.11b parameters
	5ghz	Configures 802.11a parameters
Command Default	None	
Command Modes	config apgroup	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure ATF optimization for an AP group.

```
Switch#configure terminal
Switchconfig# ap group testap
Switchconfig-apgroup# airtime-fairness dot11 24ghz optimization
```

airtime-fairness dot11 policy

To override a globally applied policy on a WLAN AP group, use the **airtime-fairness dot11 policy** command. Use the **no** form of the command to disable applied policy override.

airtime-fairness dot11 {24ghz|5ghz} **policy** *policy-name*

no airtime-fairness dot11 {24ghz|5ghz} **policy** *policy-name*

Syntax Description	24ghz	Configures 2.4 GHz airtime-fairness policy
	5ghz	Configures 5 GHz airtime-fairness policy
	<i>policy-name</i>	name of the airtime-fairness policy to assign

Command Default None

Command Modes config wlan apgroup

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines None

This example shows how to override applied policy on a WLAN AP group.

```
Switchconfig#ap group testapgroup
Switch(config-apgroup)# wlan testwlan
Switch(config-wlan-apgroup)# airtime-fairness dot11 24ghz policy testpolicy
```

airtime-fairness policy (wlan)

To configure the ATF policy for a WLAN, use the **airtime-fairness policy** command.

airtime-fairness policy *policy-name*

Syntax Description	<i>policy-name</i>	Enter the policy name.
Command Default	None	
Command Modes	config wlan	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure the ATF policy for a WLAN.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#wlan wlan-name
Switch(config-wlan)#airtime-fairness policy policy-name
```

ap dot11 rf-profile

To configure an RF-Profile for a selected band, use the **ap dot11 rf-profile** command. To delete an RF-Profile, use the **no** form of this command.

ap dot11 {24GHz | 5GHz} **rf-profile** *profile name*

Syntax Description	24ghz	Displays the 2.4-GHz band
	5ghz	Displays the 5-GHz band
	<i>profile name</i>	Name of the RF profile
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1 This command was introduced.	
Usage Guidelines	None	

This example shows how to configure an RF profile for a selected band.

```
Switch#ap dot11 24GHz rf-profile doctest
```

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 <i>pct</i>	Configures 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
data packet-count <i>count</i>	Configures 802.11 coverage minimum-failure-count threshold for uplinkdata packets.
data rssi-threshold <i>threshold</i>	Configures 802.11 minimum-receive-coverage level for voice packets.
exception global <i>percentage</i>	Configures 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
level global <i>number</i>	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 <i>percentage</i>	Configures 802.11 coverage failure rate threshold for uplink voice packets.
packet-count <i>number</i>	Configures 802.11 coverage minimum-uplink-failure count threshold for voice packets.
rssi-threshold <i>threshold</i>	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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 <i>interval</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 management 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	Parameter	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**.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.
	<i>threshold-value</i>	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	<i>number</i>	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:

```
Switch(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	<i>number</i>	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:

```
Switch(config)#ap dot11 24ghz rrm channel dca remove 11
```

ap dot11 5ghz rrm channel dca chan-width width-max

To configure the maximum allowed channel bandwidth when the best option is selected, enter the **ap dot11 5ghz rrm channel dca** *width* command.

```
ap dot11 5ghz rrm channel dca {WIDTH_20MHz | WIDTH_40MHz }
```

Syntax Description	Specifies the maximum allowed channel bandwidth limit when the best option is selected
WIDTH_20MHz	Sets the maximum channel bandwidth limit to 20 MHz.
WIDTH_40MHz	Sets the maximum channel bandwidth limit to 40 MHz.

Command Default The default channel width is 40.

Command Modes Global configuration.

Usage Guidelines None.

This example shows how to set the maximum allowed channel bandwidth limit to 40 MHz when the best option is selected, using the command:

```
Switch(config)#
```

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	Parameter	Description
	data	Specifies 802.11 coverage hole-detection data packets.
	fail-percentage <i>percentage</i>	Specifies 802.11 coverage failure-rate threshold for uplink data packets. The range is between 1 and 100
	packet-count <i>count</i>	Specifies 802.11 coverage minimum-failure-count threshold for uplink data packets.
	rssi-threshold <i>threshold</i>	Specifies 802.11 minimum-receive-coverage level for voice packets.
	exceptional global <i>value</i>	Specifies 802.11 Cisco APs coverage-exception level. The range is between 0 and 100 percent.
	level global <i>value</i>	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 <i>percentage</i>	Specifies 802.11 coverage failure rate threshold for uplink voice packets.
	packet-count <i>packet-count</i>	Specifies 802.11 coverage minimum-uplink-failure count threshold for voice packets.
	rssi-threshold <i>threshold</i>	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 switch 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 switch 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 switch 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.

```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(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	<i>controller-name</i>	Specifies the name of the controller to be added.
	<i>controller-ip</i>	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

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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	Parameter	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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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	<i>value</i> 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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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|oncepower-level}
noap dot11 {24ghz|5ghz} rrm txpower {auto|max powerLevel|min powerLevel|oncepower-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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ap dot11 5ghz rrm txpower once
```

ap dot11 airtime-fairness mode

To enable AirTime-Fairness in Enforce policy or Monitor mode, use the **ap dot11 airtime-fairness mode** command. To disable Enforce policy or Monitor mode in AirTime Fairness, use the **no** form of the command.

ap dot11 {24ghz|5ghz} airtime-fairness mode {enforce-policy|monitor}

no ap dot11 {24ghz|5ghz} airtime-fairness mode {enforce-policy|monitor}

Syntax Description	24ghz	Configures 802.11b parameters
	5ghz	Configures 802.11a parameters
	enforce-policy	Configure airtime-fairness in enforce-policy mode
	monitor	Configure airtime-fairness in monitor mode
Command Default	None	
Command Modes	Global Configuration	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.
Usage Guidelines	None	

This example shows all the parameters available for **AirTime Fairness mode**.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ap dot11 24ghz airtime-fairness mode ?
  enforce-policy  Configure airtime-fairness in enforce-policy mode
  monitor         Configure airtime-fairness in monitor mode
```

ap dot11 airtime-fairness policy-name

To create a new Air Time Fairness (ATF) policy, use the **ap dot11 airtime-fairness policy-name** command.

ap dot11 airtime-fairness policy-name *policy-name* *policy-id*

Syntax Description	<i>policy-name</i>	Enter the ATF policy name.
	<i>policy-id</i>	Enter ATF policy ID to create new policy.
Command Default	None	
Command Modes	Global Configuration	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1 This command was introduced.	

Usage Guidelines All ATF policies require a policy weight value. To add the policy weight use the **policy weight** command in config-airtime-fairness policy mode. If no policy weight is added, default value of 10 is applied. For more information about adding policy weight, see [policy-weight, on page 693](#).

This example shows .

```
Switch#ap dot11 airtime-fairness policy-name testpolicy 12
```

policy-weight

To apply policy weight to an Air Time Fairness (ATF) policy, use the **policy-weight** command.

policy-weight *policy-weight*

Syntax Description	<i>policy-weight</i>	Policy weight for ATF policy. The range is from 5 to 100. Default is 10.
Command Default	None	
Command Modes	config-airtime-fairness policy	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1 This command was introduced.	

Usage Guidelines If you do not apply a policy to the WLAN, then the default policy (with ID 0) with the policy weight of 10 is applied automatically. For more information about ATF policy creation, see [ap dot11 airtime-fairness policy-name, on page 693](#).

This example shows how to apply policy weight to an ATF policy.

```
Switch#ap dot11 airtime-fairness policy-name testpolicy 12
Switch(config-airtime-fairness policy)# policy-weight 35
```

ap group

To configure an ap group, use the **ap group** command.

ap group *group-name*

Syntax Description	<i>group-name</i>	Name of the AP group.
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure an ap group.

```
Switchconfig# ap group docgroup
```

ap name dot11 airtime-fairness mode

To enable Air Time-Fairness in Enforce policy or Monitor mode for a specific AP, use the **ap namedot11 airtime-fairness mode** command. Use **no** form of the command to disable Air Time-Fairness from either of the two modes for a specific AP.

ap name *ap-name* **dot11** {24ghz|5ghz} **airtime-fairness mode** {enforce-policy|monitor}

ap name *ap-name* **no dot11** {24ghz|5ghz} **airtime-fairness mode** {enforce-policy|monitor}

Syntax Description		
	<i>ap-name</i>	Enter access point name
	24ghz	Configures 802.11b parameters
	5ghz	Configures 802.11a parameters
	enforce-policy	Configure airtime-fairness in enforce-policy mode
	monitor	Configure airtime-fairness in monitor mode

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines None

This example shows how to disable Air Time-Fairness from either enforce-policy or monitor mode for a specific AP.

```
Switch# ap name testap no dot11 24ghz airtime-fairness mode
```

ap name dot11 airtime-fairness optimization

To enable ATF optimization for a specific AP, use the **ap name dot11 airtime-fairness optimization** command. Use **no** to disable ATF optimization for a specific AP.

ap name *ap-name* dot11 {24ghz|5ghz} airtime-fairness optimization

ap name *ap-name* no dot11 {24ghz|5ghz} airtime-fairness optimization

Syntax Description	
<i>ap-name</i>	Enter access point name
24ghz	Configures 802.11b parameters
5ghz	Configures 802.11a parameters

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows how to enable ATF optimization for a specific AP.

```
Switch#ap name doctestap dot11 24ghz airtime-fairness optimization
```

ap name no dot11 airtime-fairness wlan-name policy-name

To disable the ATF policy override on WLAN specific to a WLAN, use the **ap name no dot11 airtime-fairness wlan-name** command.

ap name *ap-name* **no dot11** {24ghz|5ghz} **airtime-fairness wlan-name** *wlan-name*

Syntax Description		
	<i>ap-name</i>	Enter access point name
	24ghz	Configures 802.11b parameters
	5ghz	Configures 802.11a parameters
	wlan-name	Configure the airtime-fairness policy for this WLAN under Cisco AP
	<i>wlan-name</i>	Enter the wlan profile name

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines None

This example shows how to disable ATF policy override on WLAN specific to a WLAN .

```
Switch#ap name testap no dot11 24ghz airtime-fairness wlan-name testwlan
```

ap name dot11 airtime-fairness wlan-name policy

To override the ATF policy on WLAN specific to one AP, use the **ap name dot11 airtime-fairness wlan-name policy-name** command.

ap name *ap-name* **dot11** {**24ghz**|**5ghz**} **airtime-fairness** **wlan-name** *wlan-name* **policy-name** *policy-name*

Syntax Description		
	<i>ap-name</i>	Access Point name
	24ghz	Configures 802.11b parameters
	5ghz	Configures 802.11a parameters
	wlan-name	Configure the airtime-fairness policy for this wlan under Cisco
	<i>wlan-name</i>	Enter the wlan profile name
	policy-name	Configure airtime-fairness policy
	<i>policy-name</i>	Enter the airtime-fairness profile name

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines None

This example shows how to override the ATF policy on WLAN specific to one AP.

```
Switch# ap name testap dot11 24ghz airtime-fairness wlan-name testwlan policy-name testpolicy
```

band-select client

To configure the client threshold minimum dB for the selected band, use the **band-select client** command. To reset the client threshold minimum dB for the selected band, use the **no** form of this command.

band-select client { **mid-rssi** | **rssi** } *dBm value*

Syntax Description	Parameter	Description
	mid-rssi	Minimum dBm of a client RSSI start to respond to probe
	rssi	Minimum dBm of a client RSSI to respond to probe
	<i>dBm value</i>	Minimum dBm of a client RSSI to respond to probe. Valid range is between -90 and -20 dBm.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines This command is enabled only for 2.4-GHz band.

This example shows how to set the client threshold to minimum dB for a selected band.

```
Switch(config-rf-profile)#band-select client rssi -50
```

band-select cycle

To configure the band cycle parameters, use the **band-select cycle** command. To reset the threshold value, use the **no** form of this command.

band-select cycle { **count** | **threshold** } *value*

Syntax Description	Parameter	Description
	count	Sets the Band Select probe cycle count.
	<i>value</i>	Maximum number of cycles not responding. The range is between 1 and 10.
	threshold	Sets the time threshold for a new scanning cycle.
	<i>value</i>	Set the threshold value in milliseconds. The valid is between 1 and 1000.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure the probe cycle count in an RF profile for a selected band.

```
Switch(config-rf-profile)#band-select cycle count 5
```

band-select expire

To configure the expiry time for the RF profile for the selected band, use the **band-select expire** command. To reset the value, use the **no** form of this command.

```
band-select expire { dual-band | suppression } value
no band-select expire { dual-band | suppression }
```

Syntax Description	Parameter	Description
	dual-band	Configures the RF Profile Band Select Expire Dual Band.
	<i>value</i>	Setting the time to expire for pruning previously known dual-band clients. The range is between 10 and 300.
	suppression	Configures the RF Profile Band Select Expire Suppression.
	<i>value</i>	Setting the time to expire for pruning previously known 802.11b/g clients. The range is between 10 and 200.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure the time to expire for a dual-band of an RF profile in a selected band.

```
Switch(config-rf-profile)#band-select expire dual-band 15
```

band-select probe-response

To configure the probe responses to the clients for a selected band, use the **band-select probe-response** command. To disable the probe-response, use the **no** form of this command.

band-select probe-response

Syntax Description	probe-response	Probe responses to clients.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	
	This example shows how to enable probe response to the clients.	
	<code>Switch(config-rf-profile)#band-select probe-response</code>	

channel

To configure a channel for the RF profile DCA channel list, use the **channel** command. To disable the channel, use the **no** form of this command.

channel { **add** | **remove** } *channel-number*

Syntax Description	add	Adds channel to the RF Profile DCA channel list.
	remove	Removes the channel from the RF Profile DCA channel list.
	<i>channel-number</i>	Channel number.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to add a channel to the RF profile DCA channel list.

```
Switch(config-rf-profile)#channel add 3
```

channel foreign

To configure the RF Profile DCA foreign AP contribution, use the **channel foreign** command. To disable the DCA Foreign AP Contribution, use the **no** form of this command.

channel foreign

Syntax Description	foreign	Configures the RF Profile DCA foreign AP contribution.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure the RF profile DCA foreign AP contribution.

```
Switch(config-rf-profile)#channel foreign
```

channel width

To configure the RF Profile DCA channel bandwidth, use the **channel width** command. To revert to default value, use the **no** form of this command.

channel width {20 |40 |80 |best}

Syntax Description		
	20	Channel width in MHz
	40	Channel width in MHz
	80	Channel width in MHz
	160	Channel width in MHz
	best	Channel width in MHz

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines This command is enabled only on 5-GHz band.

This example shows how to configure the channel bandwidth to 40 MHz.

```
Switch(config-rf-profile)#channel chan-width 40
```

coverage

To configure the voice and data coverage, use the **coverage** command. To reset the minimum RSSI value use the **no** form of this command.

coverage {**data** |**voice**} **rsi threshold** *value*

Syntax Description	data	Configure Coverage Hole Detection for data packets.
	voice	Configure Coverage Hole Detection for voice packets.
	<i>value</i>	Minimum RSSI value for the packets received by the access point. The valid range is between -90 and -60 dBm.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure the coverage hole detection for data packets.

```
Switch(config-rf-profile)#coverage data rssi threshold -85
```

coverage exception

To configure the Cisco AP coverage exception level, use the **coverage exception** command. To reset the exception-level percentage use the **no** form of this command.

coverage exception *exception-level*

Syntax Description	<i>exception-level</i>	Cisco AP coverage exception level with valid range between 0 and 100 percent.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to set the Cisco AP coverage exception level.

```
Switch(config-rf-profile)#coverage exception 70
```

coverage level

To configure Cisco AP client minimum coverage level, use the **coverage level** command. To reset the coverage client value use the **no** form of this command.

coverage level *clients*

Syntax Description	<i>clients</i>	Minimum coverage level. Range is between 1 and 200 clients.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure the Cisco AP client minimum level.

```
Switch(config-rf-profile)#coverage level 180
```

clear wireless airtime-fairness statistics

To clear the wireless airtime-fairness statistics, use the **clear wireless airtime-fairness statistics** command.

clear clear wireless airtime-fairness statistics

Syntax Description	airtime-fairness	Clears the airtime-fairness statistics
---------------------------	-------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows how to clear the wireless airtime-fairness statistics.

```
Switch#clear wireless airtime-fairness statistics
```

dot11n-only

To enable 802.11n client only mode of the RF profile, use the **dot11n-only** command. To disable the 802.11n client only mode use the **no** form of this command.

dot11n-only

Syntax Description	dot11n-only	802.11n client only mode of the RF Profile.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to enable 802.11n client only mode of the RF Profile.

```
Switch(config-rf-profile) #dot11n-only
```

load-balancing

To configure the RF Profile Load Balance, use the **load-balancing** command. To reset RF profile load balance value, use the **no** form of this command.

load-balancing { **denial** | **window** } *value*

Syntax Description	denial	Configures the number of load balancing denial.
	<i>value</i>	Enter the load balancing denial count. The range is between 1 and 10.
	window	Set Aggressive Load Balancing client window.
	<i>value</i>	Number of clients. The range is between 0 and 20.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure the number of load balancing denial.

```
Switch#load-balancing denial 4
```

high-density clients count

To configure the RF profile max clients, use the **high-density clients count** command. To reset the RF profile max clients use the **no** form of this command.

high-density clients count *value*

Syntax Description	<i>value</i>	Maximum client connections per AP radio. The range is between 0 and 200.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	
	This example shows how to configure the RF profile max clients.	
	<code>Switch(config-rf-profile)#high-density clients count 25</code>	

high-density clients wlan

To configure the maximum clients per AP on a WLAN, use the **high-density clients wlan** command. To reset the count use the **no** form of this command.

high-density clients wlan *wlan name* **count** *count*

Syntax Description	<i>wlan name</i>	Enter the name of the WLAN to limit clients per AP.
	<i>count</i>	Maximum client connections per AP per WLAN. The range is between 0 and 200.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure the maximum clients per AP on a WLAN

```
Switch(config-rf-profile)#high-density clients wlan doctest count 20
```

high-density multicast data-rate

To configure the value for RF profile Multicast Data Rate, use the **high-density multicast data-rate** command. To reset the data rate to auto, use the **no** form of this command.

high-density multicast data-rate

```
{RATE_12M|RATE_18M|RATE_24M|RATE_36M|RATE_48M|RATE_54M|RATE_6M|RATE_9M}
```

Syntax Description	multicast	Configures the RF Profile multicast.
	data-rate	The value for RF Profile Multicast Data Rate.
	RATE_12M	802.11 12M Rate
	RATE_18M	802.11 18M Rate
	RATE_24M	802.11 24M Rate
	RATE_36M	802.11 36M Rate
	RATE_48M	802.11 48M Rate
	RATE_54M	802.11 54M Rate
	RATE_6M	802.11 6M Rate
	RATE_9M	802.11 9M Rate

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure the value for RF profile Multicast Data Rate.

```
Switch(config-rf-profile)#high-density multicast data-rate RATE_9M
```

high-density rx-sop threshold

To configure the value for RF Profile Rx SOP threshold, use the **high-density rx-sop threshold** command. To revert the Rx SOP to auto, use the **no** form of this command.

high-density rx-sop threshold {auto |high |low |medium }

Syntax Description	Command	Description
	rx-sop	Configures the RF Profile Rx SOP threshold.
	threshold	Configures the value for RF Profile Rx SOP threshold.
	auto	Reverts radio receiver SOP threshold to auto.
	high	Sets radio receiver SOP threshold to high.
	low	Sets radio receiver SOP threshold to low.
	medium	Sets radio receiver SOP threshold to medium.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to configure radio receiver SOP threshold for an RF Profile to high.

```
Switch(config-rf-profile)#high-density rx-sop threshold high
```

rate

To configure 802.11 operational rates, use the **rate** command. To revert to the rate default state, use the **no** form of this command.

```
rate
{RATE_12M|RATE_18M|RATE_24M|RATE_36M|RATE_48M|RATE_54M|RATE_6M|RATE_9M} {disable|
mandatory|supported}
```

Syntax	Description
RATE_12M	802.11 12M Rate.
RATE_18M	802.11 18M Rate.
RATE_24M	802.11 24M Rate.
RATE_36M	802.11 36M Rate.
RATE_48M	802.11 48M Rate.
RATE_54M	802.11 54M Rate.
RATE_6M	802.11 6M Rate.
RATE_9M	802.11 9M Rate.
disable	Disables a rate.
mandatory	Configures a rate to mandatory.
supported	Configures a rate to supported.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to disable 802.11 9M operational rate.

```
Switch(config-rf-profile)#rate RATE_9M disable
```

rate mcs

To enable the RF profile MCS data rates, use the **rate mcs** command. To disable the RF profile MCS data rates use the **no** form of this command.

rate mcs *index-number*

Syntax Description	<i>index-number</i>	Enter index number of RF Profile MCS Data Rates. The range is between 0 and 31.
---------------------------	---------------------	---

Command Default	None
------------------------	------

Command Modes	config-rf-profile
----------------------	-------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	None
-------------------------	------

This example shows how to enable the RF Profile mcs data rate.

```
Switch(config-rf-profile) #rate mcs 5
```

trap threshold

To configure the RF Profile Trap Threshold parameters, use the **trap threshold** command. To revert to default value, use the **no** form of this command.

trap threshold {**clients** |**interference** |**noise** |**utilization** } *value*

Syntax Description	clients	interference	noise	utilization
	Configures the RF Profile Trap for Threshold Clients.			
	<i>value</i>	Number of clients that associate with an access point, after which the trap is sent. The range is between 1 and 200.		
		Configures the RF Profile Trap Threshold for Interference.		
		<i>value</i>	Configures the percentage value for Rf Profile Trap Threshold Interference. The range is between 0 and 100.	
			Configures the RF Profile Trap Threshold for Noise.	
			<i>value</i>	Configures the value for Rf Profile Trap Threshold Noise in dbm. The range is between -127 and 0.
				Configures the RF Profile Trap Threshold for Utilization.
				<i>value</i>
				Configures the percentage value for RF Profile Trap Threshold Utilization. The range is between 0 and 100.
Command Default	None			
Command Modes	config-rf-profile			
Command History	Release	Modification		
	Cisco IOS XE Denali 16.3.1	This command was introduced.		
Usage Guidelines	None			
	This example shows how to set the RF Profile Threshold Trap for the clients.			
	<code>Switch(config-rf-profile)#trap threshold clients 10</code>			

tx-power

To configure Tx Power levels, use the **tx-power** command. To revert to default value, use the **no** form of this command.

tx-power { **min** | **max** } *dBm value*

Syntax Description		
	max	Configures maximum Auto-RF transmit power.
	min	Configures maximum Auto-RF transmit power.
	<i>dBm value</i>	Enter value in dBm. The range is between -10 and 30.

Command Default None

Command Modes config-rf-profile

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to set the Tx power level to min.

```
Switch(config-rf-profile)#tx-power min -14
```

tx-power v1 threshold

To configure the Transmit Power Control (TPC) version 1 threshold, use the **tx-power v1 threshold** command. To revert to default dBm value, use the **no** form of this command.

tx-power v1 threshold *dBm value*

Syntax Description	<i>dBm value</i>	Transmit Power Control version 1 threshold value. The range is between –80 and –50 dBm.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	
	This example shows how to set the TPCv1 threshold to –75dBm.	
	<code>Switch#tx-power v1 threshold -75</code>	

no ap dot11 airtime-fairness policy-name

To delete a AirTime Fairness policy, use the **no ap dot11 airtime-fairness policy-name** command.

no ap dot11 airtime-fairness policy-name *policy-name*

Syntax Description	<i>policy-name</i>	Enter the airtime-fairness policy name
---------------------------	--------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines	None
-------------------------	------

This example shows how to delete a AirTime Fairness policy.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch# no ap dot11 airtime-fairness policy-name testpol
```

remote-lan

To configure an remote-lan to an ap group, use the **remote-lan** command. To delete the remote-lan from the ap group, use the **no** form of this command.

remote-lan *name*

Syntax Description	<i>name</i>	Enter the name of the remote-lan
Command Default	None	
Command Modes	config-apgroup	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to configure an remote-lan to an ap group.

```
Switch(config-apgroup)#remote-lan rlanstest
```

rf-profile dot11 24ghz

To assign the RF Profile to the 2.4GHz band AP group, use the **rf-profile dot11 24ghz** command.

rf-profile dot11 24ghz *name*

Syntax Description	<i>name</i>	Enter the name of the RF Profile to be assigned to the current AP group.
---------------------------	-------------	--

Command Default	None
------------------------	------

Command Modes	config-apgroup
----------------------	----------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	None
-------------------------	------

This example shows how to assign the RF Profile to the 2.4GHz band AP group.

```
Switch(config-apgroup)#rf-profile dot11 24ghz doctest
```

rf-profile dot11 5ghz

To assign the RF Profile to the 5GHz band AP group, use the **rf-profile dot11 5ghz** command.

rf-profile dot11 5ghz *name*

Syntax Description	<i>name</i>	Enter the name of the RF Profile to be assigned to the current AP group.
Command Default	None	
Command Modes	config-apgroup	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1 This command was introduced.	
Usage Guidelines	None	

This example shows how to assign the RF Profile to the 5GHz band AP group.

```
Switch(config-apgroup)#rf-profile dot11 24ghz doc5test
```

show ap airtime-fairness ap-group

To view ATF configuration for a specific AP group, use the **show ap airtime-fairness ap-group** command.

show ap airtime-fairness ap-group *group-name*

Syntax Description	<i>group-name</i>	Enter AP-group name
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows ATF configuration for a specific AP group .

```
Switch#show ap airtime-fairness ap-group ?
Site Description:
Airtime-fairness 2.4GHz Mode:: Disable
Airtime-fairness 2.4GHz Optimization : n/a
Airtime-fairness 5GHz Mode:: Disable
Airtime-fairness 5GHz Optimization : n/a
```

WLAN ID	WLAN Name	Interface	ATF Policy(2.4GHz)	ATF Policy(5GHz)

show ap airtime-fairness (ap)

To view ATF configuration for a specific AP, use the **show ap airtime-fairness** command.

show ap name*ap-name* **airtime-fairness**

Syntax Description	<i>ap-name</i>	Enter access point name
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows how to view ATF configuration for a specific AP.

```
Switch# show ap name testap airtime-fairness
```

show ap airtime-fairness (per radio)

To view AP list with Air Time Fairness configuration per radio, use the **show ap airtime-fairness** command.

show ap airtime-fairness

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows AP list with AirTime-Fairness per radio.

```
Switch#show ap airtime-fairness
```

show ap airtime-fairness policy (all)

To view all configured policies, use the **show ap airtime-fairness policy** command.

show ap airtime-fairness policy

Syntax Description	policy	Shows Airtime Fairness policy information
Command Default	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows all the configured airtime-fairness policies.

```
Switch#show ap airtime-fairness policy
Policy ID   Policy Name   Weight
-----
23          f             10
12          asd           10
13          pol           10
50          meaw         45
20          pocy         10
0           Default      10
```

show ap airtime-fairness wlan

To view the complete list of configured WLANs with Air Time Fairness policies applied, use the **show ap airtime-fairness wlan** command.

show ap airtime-fairness wlan

Syntax Description	wlan	Display airtime-fairness configuration for all wlangs
--------------------	------	---

Command Default	Privileged EXEC
-----------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows the complete list of configured WLANs and ATF policies applied.

```
Switch#show ap airtime-fairness wlan
```

WLAN ID	Profile Name	ATF Profile Name	Weight
12	doctestlan	Default	10

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	Parameter	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.

```
Switch#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
```

```
show ap dot11 24ghz
```

```
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	Parameter	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.

```
Switch#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
```

show ap dot11 airtime-fairness (radio bands)

To view AP list with ATF configured radio bands, use the `show ap dot11 airtime-fairness` command.

```
show ap dot11 {24ghz|5ghz} airtime-fairness
```

Syntax Description	24ghz	Show 802.11b configuration
	5ghz	Show 802.11a configuration
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.
Usage Guidelines	None	

This example shows how to view AP list with ATF configured radio bands.

```
Switch#show ap dot 24ghz airtime-fairness
```

show ap dot11 24ghz rf-profile summary

To display the 2.4GHz RF Profiles summary, use the **show ap dot11 24ghz rf-profile summary** command.

show ap dot11 24ghz rf-profile summary

Syntax Description	summary	Show RF Profiles summary.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows the 24GHz AP-Profile summary.

```
Switch(config-rf-profile)#show ap dot11 24ghz rf-profile summaryNumber of RF Profiles : 1
```

RF Profile Name	Band	Description	Applied	State
doctest	2.4 GHz		No	Down

show ap dot11 5ghz rf-profile summary

To display the 5GHz ap RF-Profiles, use the **show ap dot11 5ghz rf-profile summary** command.

show ap dot11 5ghz rf-profile summary

Syntax Description	summary	Show RF Profiles summary.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1 This command was introduced.	
Usage Guidelines	None	

This example shows how to display the 5GHz ap RF-Profile summary.

```
Switch#show ap dot11 5ghz rf-profile summary
Number of RF Profiles : 1
```

RF Profile Name	Band	Description	Applied	State
doc5test	5 GHz		No	Down

show ap name dot11 airtime-fairness summary

To view the ATF statistics for a specific AP, use the **show ap name dot11 airtime-fairness summary** command.

show ap name *ap-name* dot11 {24ghz|5ghz} airtime-fairness summary

Syntax Description	<i>ap-name</i>	Display the stats of 24GHz 5GHz airtime-fairness
	24ghz	Show 802.11b configuration
	5ghz	Show 802.11a configuration
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.
Usage Guidelines	None	

This example shows how to view the ATF statistics for a specific AP.

```
Switch#show ap ame testap dot11 24ghz airtime-fairness summary
```

show ap name dot11 airtime-fairness policy statistics

To view statistics for each ATF policy, use the **show ap name dot11 airtime-fairness policy statistics** command.

show ap name *ap-name* **dot11** {**24ghz**|**5hz**} **airtime-fairness policy** *policy-name* **statistics**

Syntax Description	<i>ap-name</i>	Enter access point name
	24ghz	Show 802.11b configuration
	5hz	Show 802.11a configuration
	<i>policy-name</i>	Enter policy name
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1	This command was introduced.

This example shows how to view statistics for each ATF policy.

```
Switch#show ap name testap dot11 24ghz airtime-fairness policy testpolicy statistics
```

show ap name dot11 airtime-fairness wlan name statistics

To view ATF statistics per WLAN active on specific AP, use the **show ap name dot11 airtime-fairness wlan name statistics** command.

show ap name dot11 {24ghz|5ghz} airtime-fairness wlan name *wlan-name* statistics

Syntax Description	name	Display airtime-fairness stats by profile name
	<i>wlan-name</i>	Enter WLAN name
	statistics	Display the stats of 24GHz 5GHz airtime-fairness
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.1 This command was introduced.	

This example shows how to view ATF statistics per WLAN active on specific AP.

```
Switch#show ap name testap dot11 24ghz airtime-fairness wlan name testwlan statistics
```

show ap rf-profile summary

To display the ap RF-Profile summary, use the **show ap rf-profile summary** command.

show ap rf-profile summary

Syntax Description	summary	Show summary of RF Profiles
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to display the ap RF-Profile summary .

```
Switch#show ap rf-profile summary
Number of RF Profiles : 1
```

RF Profile Name	Band	Description	Applied	State
doctest	2.4 GHz		No	Down

show ap rf-profile name

To display the selected ap RF-Profile details, use the **show ap rf-profile name** command.

show ap rf-profile name *profile-name* **detail**

Syntax Description		
	<i>profile-name</i>	Name of the RF-Profile.
	detail	Show detail of selected RF Profile.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines None

This example shows how to display the details of the selected RF-Profile.

```
Switch#show ap rf-profile name doctest detail
Description :
AP Group Names :
RF Profile Name : doctest
Band : 2.4 GHz
802.11n client only : Disabled
Transmit Power Threshold v1: -70 dBm
Min Transmit Power: -10 dBm
Max Transmit Power: 30 dBm
Operational Rates
 802.11b 1M Rate : Mandatory
 802.11b 2M Rate : Mandatory
 802.11b 5.5M Rate : Mandatory
 802.11b 11M Rate : Mandatory
 802.11b 6M Rate : Mandatory
 802.11b 9M Rate : Supported
 802.11b 12M Rate : Supported
 802.11b 18M Rate : Supported
 802.11b 24M Rate : Supported
 802.11b 36M Rate : Supported
 802.11b 48M Rate : Supported
 802.11b 54M Rate : Supported
Max Clients : 200
Wlan name                               Max Clients
-----
Trap Threshold
  Clients: 12 clients
  Interference: 10%
  Noise: -70 dBm
  Utilization: 80%
Multicast Data Rate: auto
Rx SOP Threshold : auto
Band Select
```

```
Probe Response: Disabled
Cycle Count: 2 cycles
Cycle Threshold: 200 milliseconds
Expire Suppression: 20 seconds
Expire Dual Band: 60 seconds
Client RSSI: -80 dBm
Client Mid RSSI: -80 dBm
Load Balancing
Window: 5 clients
Denial: 3 count
Coverage Data
Data: -80 dBm
Voice: -80 dBm
Minimum Client Level: 3 clients
Exception Level: 25%
DCA Channel List : 1,5,9,13
DCA Foreign AP Contribution : Enabled
802.11n MCS Rates
MCS 0 : Enabled
MCS 1 : Enabled
MCS 2 : Enabled
MCS 3 : Enabled
MCS 4 : Enabled
MCS 5 : Enabled
MCS 6 : Enabled
MCS 7 : Enabled
MCS 8 : Enabled
MCS 9 : Enabled
MCS 10 : Enabled
MCS 11 : Enabled
MCS 12 : Enabled
MCS 13 : Enabled
MCS 14 : Enabled
MCS 15 : Enabled
MCS 16 : Enabled
MCS 17 : Enabled
MCS 18 : Enabled
MCS 19 : Enabled
MCS 20 : Enabled
MCS 21 : Enabled
MCS 22 : Enabled
MCS 23 : Enabled
MCS 24 : Enabled
MCS 25 : Enabled
MCS 26 : Enabled
MCS 27 : Enabled
MCS 28 : Enabled
MCS 29 : Enabled
MCS 30 : Enabled
MCS 31 : Enabled
State : Down
```

show wireless mobility controller ap

To display the list of access points which have joined the sub-domain, use the **wireless mobility controller ap** command.

show wireless mobility controller ap

Syntax Description	ap	Show joined Access Point in sub-domain.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to list the access points which have joined the sub-domain.

```
Switch#show wireless mobility controller ap
Number of AP entries in the sub-domain      : 2
```

AP name	AP radio MAC	Controller IP	Location
bos2kk	00f2.8c42.f520	default-group	default-group
IosAP1	34ed.522f.7e60	default-group	default-group

shutdown

To close the RF Profile and disable the network, use the **shutdown** command. To disable shutdown execution, use the **no** form of this command.

shutdown

Syntax Description	shutdown	Shuts down the profile and disables network.
Command Default	None	
Command Modes	config-rf-profile	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	

This example shows how to close a RF Profile and disable the network.

```
Switch(config-rf-profile)#shutdown
```

wlan

To configure an WLAN to an ap group, use the **wlan** command. To delete the WLAN from the ap group, use the **no** form of this command.

wlan *wlan-name*

Syntax Description	<i>wlan-name</i>	Enter the name of the WLAN to be configured to an AP group.
Command Default	None	
Command Modes	config-apgroup	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.
Usage Guidelines	None	
	This example shows how to configure an WLAN to an ap group.	
	Switch(config-apgroup)# wlan docwlan	



PART **X**

Security

- [Security](#), on page 749



Security

- [aaa accounting dot1x, on page 752](#)
- [aaa accounting identity, on page 754](#)
- [aaa authentication dot1x, on page 756](#)
- [aaa authorization, on page 757](#)
- [aaa new-model, on page 761](#)
- [access-session mac-move deny, on page 763](#)
- [action, on page 765](#)
- [authentication host-mode, on page 766](#)
- [authentication mac-move permit, on page 768](#)
- [authentication priority, on page 770](#)
- [authentication violation, on page 773](#)
- [auto security, on page 775](#)
- [auto security-port, on page 776](#)
- [cisp enable, on page 777](#)
- [clear errdisable interface vlan, on page 778](#)
- [clear mac address-table, on page 779](#)
- [debug ip rip, on page 781](#)
- [deny \(MAC access-list configuration\), on page 783](#)
- [device-role \(IPv6 snooping\), on page 787](#)
- [device-role \(IPv6 nd inspection\), on page 788](#)
- [device-tracking policy, on page 789](#)
- [dot1x critical \(global configuration\), on page 791](#)
- [dot1x max-start, on page 792](#)
- [dot1x pae, on page 793](#)
- [dot1x supplicant force-multicast, on page 794](#)
- [dot1x test eapol-capable, on page 795](#)
- [dot1x test timeout, on page 796](#)
- [dot1x timeout, on page 797](#)
- [epm access-control open, on page 799](#)
- [ip admission, on page 800](#)
- [ip admission name, on page 801](#)
- [ip device tracking maximum, on page 803](#)
- [ip device tracking probe, on page 804](#)

- ip dhcp snooping database, on page 805
- ip dhcp snooping information option format remote-id, on page 807
- ip dhcp snooping verify no-relay-agent-address, on page 808
- ip source binding, on page 809
- ip verify source, on page 810
- ipv6 snooping policy, on page 812
- limit address-count, on page 813
- mab request format attribute 32, on page 814
- match (access-map configuration), on page 816
- authentication logging verbose, on page 818
- dot1x logging verbose, on page 819
- mab logging verbose, on page 820
- permit (MAC access-list configuration), on page 821
- protocol (IPv6 snooping), on page 825
- radius server, on page 826
- router rip, on page 828
- security level (IPv6 snooping), on page 829
- security passthru, on page 830
- show aaa clients, on page 831
- show aaa command handler, on page 832
- **show aaa local**, on page 833
- show aaa servers, on page 834
- show aaa sessions, on page 835
- show authentication history, on page 836
- show authentication sessions, on page 837
- show auto security, on page 840
- show cisp, on page 842
- show dot1x, on page 844
- show eap pac peer, on page 846
- show ip dhcp snooping statistics, on page 847
- show ip rip database, on page 850
- show radius server-group, on page 852
- show storm-control, on page 854
- show vlan access-map, on page 856
- show vlan filter, on page 857
- show vlan group, on page 858
- storm-control, on page 859
- switchport port-security aging, on page 862
- switchport port-security mac-address, on page 864
- switchport port-security maximum, on page 867
- switchport port-security violation, on page 869
- tracking (IPv6 snooping), on page 871
- trusted-port, on page 873
- wireless dot11-padding, on page 874
- wireless security dot1x, on page 875
- wireless security lsc, on page 877

- wireless security strong-password, on page 878
- wireless wps ap-authentication, on page 879
- wireless wps auto-immune, on page 880
- wireless wps cids-sensor, on page 881
- wireless wps client-exclusion, on page 882
- wireless wps mfp infrastructure, on page 884
- wireless wps rogue, on page 885
- wireless wps shun-list re-sync, on page 886
- vlan access-map, on page 887
- vlan filter, on page 889
- vlan group, on page 890

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: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. <p>The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.</p>
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:

```
Switch(config)# aaa new-model  
Switch(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: <ul style="list-style-type: none"> • name — Name of a server group. • radius — Lists of all RADIUS hosts. • tacacs+ — Lists of all TACACS+ hosts. <p>The group keyword is optional when you enter it after the broadcast group and group keywords. You can enter more than optional group keyword.</p>
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:

```
Switch# 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.

```
Switch# configure terminal
```

```
Switch(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	<p>default The default method when a user logs in. Use the listed authentication method that follows this argument.</p> <hr/> <p><i>method1</i> Specifies the server authentication. Enter the group radius keywords to use the list of all RADIUS servers for authentication.</p> <p>Note Though other keywords are visible in the command-line help strings, only the default and group radius keywords are supported.</p>
---------------------------	---

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	<p>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.</p>
-------------------------	---

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.

```
Switch(config)# aaa new-model
Switch(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.
<i>level</i>	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.
<i>list_name</i>	Character string used to name the list of authorization methods.
<i>method1</i> [<i>method2</i> ...]	(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** and **tacacs server** 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 <i>group-name</i>	Uses a cache server group for authorization.

Keyword	Description
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group <i>group-name</i> 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.

```
Switch(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 3.2SE	This command was introduced.

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
!
```

Examples

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 switch, 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 switch. 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 switch:

```
Switch(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.

Command	Description
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.

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 a12:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address a12
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(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	multi-domain	multi-host	single-host
	Enables multiple-authorization mode (multi-auth mode) on the port.	Enables multiple-domain mode on the port.	Enables multiple-host mode on the port.	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:

```
Switch(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Switch(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Switch(config-if) # authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Switch(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 switch, 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 disabled.

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 switch. 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 switch:

```
Switch(config)# authentication mac-move permit
```

Related Commands

Command	Description
access-session mac-move deny	Disables MAC move on a switch.
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.

Command	Description
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	<p>dot1x (Optional) Adds 802.1x to the order of authentication methods.</p> <hr/> <p>mab (Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.</p> <hr/> <p>webauth Adds web authentication to the order of authentication methods.</p>				
Command Default	The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.				
Command Modes	Interface configuration				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>Ordering sets the order of methods that the switch attempts when trying to authenticate a new device is connected to a port.</p> <p>When configuring multiple fallback methods on a port, set web authentication (webauth) last.</p> <p>Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.</p>				
 Note	<p>If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.</p> <hr/> <p>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.</p> <p>This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:</p> <pre>Switch(config-if)# authentication priority dotx webauth</pre> <p>This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:</p>				

```
Switch(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.

Command	Description
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.
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	Mode	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:

```
Switch(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:

```
Switch(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:

```
Switch(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:

```
Switch(config-if)# authentication violation replace
```

You can verify your settings by entering the **show authentication** privileged EXEC command.

auto security

To configure global auto security, use the **auto security** command in global configuration mode. To disable auto security, use the **no** form of this command.

auto security
no auto security

This command has no arguments and keywords.

Command Default

Auto security is enabled globally.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines

When you configure auto security in global configuration mode, auto security is enabled on all interfaces. When you disable auto security, it is disabled on all interfaces.

To enable auto security on specific interfaces, use the **auto security-port** command in interface configuration mode.



Note

In Cisco IOS Release 15.2(5)E, auto security is enabled on interfaces, when the **auto security** command is configured in global configuration mode; however, the **auto security-port {host | uplink}** command is not explicitly saved to the interface configuration. When auto security is configured on an interface, and then the **auto security-port {host | uplink}** command is removed from that interface; the **no auto security-port {host | uplink}** command is saved to interface configuration.

This example shows how to enable auto security globally:

```
Switch(config)# auto security
```

Related Commands

Command	Description
auto security-port	Configures auto security on an interface.
show auto security	Displays auto security status.

auto security-port

To configure auto security on an interface, use the **auto security-port** command in interface configuration mode. To disable auto security on an interface, use the **no** form of this command.

```
auto security {host |uplink}
no auto security
```

Syntax Description

host	Configures auto security for a host port.
uplink	Configures auto security for an uplink port.

Command Default

Auto security is disabled on all interfaces.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines

You can enable auto security globally, by using the **auto security** in global configuration mode.



Note

In Cisco IOS Release 15.2(5)E, auto security is enabled on interfaces, when the **auto security** command is configured in global configuration mode; however, the **auto security-port {host |uplink}** command is not explicitly saved to the interface configuration. When auto security is configured on an interface, and then the **auto security-port {host |uplink}** command is removed from that interface; the **no auto security-port {host |uplink}** command is saved to interface configuration.

The following example shows how to configure auto security on an interface:

```
Switch(config)# interface gigabitethernet 1/0/2
Switch(config-if)# auto security-port host
```

Related Commands

Command	Description
auto security	Configures global auto security.
show auto security	Displays auto security status.

cisp enable

To enable Client Information Signaling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch and a supplicant to an authenticator switch, use the **cisp enable** global configuration command.

cisp enable
no cisp enable

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x

Usage Guidelines The link between the authenticator and supplicant switch is a trunk. When you enable VTP on both switches, the VTP domain name must be the same, and the VTP mode must be server.

To avoid the MD5 checksum mismatch error when you configure VTP mode, verify that:

- VLANs are not configured on two different switches, which can be caused by two VTP servers in the same domain.
- Both switches have different configuration revision numbers.

This example shows how to enable CISP:

```
Switch(config)# cisp enable
```

Related Commands	Command	Description
	dot1x credentials <i>profile</i>	Configures a profile on a supplicant switch.
	dot1x supplicant force-multicast	Forces 802.1X supplicant to send multicast packets.
	dot1x supplicant controlled transient	Configures controlled access by 802.1X supplicant.
	show cisp	Displays CISP information for a specified interface.

clear errdisable interface vlan

To reenab 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	<i>interface-id</i>	Specifies an interface.
	<i>vlan list</i>	(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 reenab 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 reenab all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Switch# 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 <i>mac-addr</i>		(Optional) Deletes the specified dynamic MAC address.
interface <i>interface-id</i>		(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.
vlan <i>vlan-id</i>		(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:

```
Switch# 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.

Command	Description
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.

debug ip rip

To display information on Routing Information Protocol (RIP) routing transactions, use the **debug ip rip** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

```
debug ip rip [{database |events |trigger}]
no debug ip rip [{database |events |trigger}]
```

Syntax Description

database	(Optional) Displays information about RIP database events.
events	(Optional) Displays information about RIP protocol-based events.
trigger	(Optional) Displays information about RIP trigger extensions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E2	This command was introduced.

Examples

In the following example, the router being debugged has received updates from a router at source address 10.89.80.28. In this scenario, information has been sent to about five destinations in the routing table update. Notice that the fourth destination address in the update, 172.31.0.0, is inaccessible because it is more than 15 hops away from the router from which the update was sent. The router being debugged also sends updates, in both cases to broadcast address 255.255.255.255 as the destination.

```
Device# debug ip rip

RIP: received update from 10.89.80.28 on GigabitEthernet0/0/0
 10.89.95.0 in 1 hops
 10.89.81.0 in 1 hops
 10.89.66.0 in 2 hops
 172.31.0.0 in 16 hops (inaccessible)
 0.0.0.0 in 7 hop
RIP: sending update to 255.255.255.255 via GigabitEthernet0/0/0 (10.89.64.31)
 subnet 10.89.94.0, metric 1
 172.31.0.0 in 16 hops (inaccessible)
RIP: sending update to 255.255.255.255 via Serial1 (10.89.94.31)
 subnet 10.89.64.0, metric 1
 subnet 10.89.66.0, metric 3
 172.31.0.0 in 16 hops (inaccessible)
 default 0.0.0.0, metric 8
```

The second line is an example of a routing table update. It shows the number of hops between a given Internet address and the device.

The entries show that the device is sending updates that are similar, except that the number in parentheses is the source address encapsulated into the IP header.

The following are examples for the **debug ip rip** command of entries that appear at startup, during an interface transition event, or when a user manually clears the routing table:

```
RIP: broadcasting general request on GigabitEthernet0/0/0  
RIP: broadcasting general request on GigabitEthernet1/0/0
```

The following entry is most likely caused by a malformed packet from the sender:

```
RIP: bad version 128 from 160.89.80.43
```

Related Commands

Command	Description
show ip rip database	Displays summary address entries in the RIP routing database entries if relevant are routes being summarized based upon a summary address.

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 | larc-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 | larc-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 <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	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 <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	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.
<i>type mask</i>	(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.
lavr-sca	(Optional) Specifies EtherType DEC-LAVR-SCA.
lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. <i>mask</i> 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 <i>cos</i>	(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.

```
Switch(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:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Switch(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.

Command	Description
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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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.
	Cisco IOS XE Denali 16.3.1	The keywords monitor and router are deprecated.

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:

```
Switch(config)# ipv6 nd inspection policy policy1
Switch(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	<i>policy-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.1.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.1.1	This command was introduced.
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:

```
Switch(config)# device-tracking policy policy1  
Switch(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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch(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	<i>number</i> 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:

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x max-start 5
```

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

Syntax Description	supplicant	authenticator
	The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.	The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.

Command Default PAE type is not set.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x

Usage Guidelines Use the **no dot1x pae** interface configuration command to disable IEEE 802.1x authentication on the port. When you configure IEEE 802.1x authentication on a port, such as by entering the **dot1x port-control** interface configuration command, the switch automatically configures the port as an IEEE 802.1x authenticator. After the **no dot1x pae** interface configuration command is entered, the Authenticator PAE operation is disabled.

The following example shows that the interface has been set to act as a supplicant:

```
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x pae supplicant
```

dot1x supplicant force-multicast

To force a supplicant switch to send only multicast Extensible Authentication Protocol over LAN (EAPOL) packets whenever it receives multicast or unicast EAPOL packets, use the **dot1x supplicant force-multicast** command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x supplicant force-multicast
no dot1x supplicant force-multicast

Syntax Description	This command has no arguments or keywords.	
Command Default	The supplicant switch sends unicast EAPOL packets when it receives unicast EAPOL packets. Similarly, it sends multicast EAPOL packets when it receives multicast EAPOL packets.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x

Usage Guidelines Enable this command on the supplicant switch for Network Edge Access Topology (NEAT) to work in all host modes.

This example shows how force a supplicant switch to send multicast EAPOL packets to the authenticator switch:

```
Switch(config)# dot1x supplicant force-multicast
```

Related Commands	Command	Description
	cisp enable	Enable Client Information Signalling Protocol (CISP) on a switch so that it acts as an authenticator to a supplicant switch.
	dot1x credentials	Configure the 802.1x supplicant credentials on the port.
	dot1x pae supplicant	Configure an interface to act only as a supplicant.

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 <i>interface-id</i>	(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:

```
Switch# 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 <i>timeout</i>	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	<i>timeout</i>	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:

```
Switch# 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 [<i>interface interface-id</i>]	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 <i>seconds</i>	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 <i>seconds</i>	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 <i>seconds</i>	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 <i>seconds</i>	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). <ul style="list-style-type: none"> 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 <i>seconds</i>	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. <ul style="list-style-type: none"> The range is from 1 to 65535. The default is 30. <p>If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.</p>
start-period <i>seconds</i>	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. In Cisco IOS Release 15.2(5)E, this command is only available in the supplicant mode. If the command is applied in any other mode, the command misses from the configuration.

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:

```
Switch(config)# configure terminal
Switch(config)# interface g1/0/3
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(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.

```
Switch(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:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet1/0/1
Switch(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.

```
Switch# configure terminal
Switch(config)# fallback profile profile1
Switch(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

<i>name</i>	Name of network admission control rule.
consent	Associates an authentication proxy consent web page with the IP admission rule specified using the <i>admission-name</i> argument.
proxy http	Configures web authentication custom page.
absolute-timer <i>minutes</i>	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time <i>minutes</i>	(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).
<i>acl</i>	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.
<i>acl-name</i>	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.
<i>service-policy-name</i>	Control plane tag service policy that is configured using the policy-map type control tag <i>policyname</i> 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.

Examples

This example shows how to configure only web authentication on a switch port:

```
Switch# configure terminal
Switch(config) ip admission name http-rule proxy http
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip access-group 101 in
Switch(config-if)# ip admission rule
Switch(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Switch# configure terminal
Switch(config)# ip admission name rule2 proxy http
Switch(config)# fallback profile profile1
Switch(config)# ip access group 101 in
Switch(config)# ip admission name rule2
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x fallback profile1
Switch(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.
fallback profile	Creates a web authentication fallback profile.
ip admission	Enables web authentication on a port.
show authentication sessions interface <i>interface</i> 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	<i>number</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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.



Note This command enables IPDT wherever its configured

Examples

This example shows how to configure IP device tracking parameters on a Layer 2 access port:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(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 <i>number</i>	Sets the number of times that the switch sends the ARP probe. The range is from 1 to 255.
delay <i>seconds</i>	Sets the number of seconds that the switch waits before sending the ARP probe. The range is from 1 to 120.
interval <i>seconds</i>	Sets the number of seconds that the switch 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.

Examples	
	This example shows how to set SVI as the source for ARP probes:
	<pre>Switch(config)# ip device tracking probe use-svi</pre>

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:

```
Switch(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:

```
Switch(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:

```
Switch(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 reenale verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Switch(config)# no ip dhcp snooping verify no-relay-agent-address
```

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	<i>mac-address</i>	Binding MAC address.
	vlan <i>vlan-id</i>	Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.
	<i>ip-address</i>	Binding IP address.
	interface <i>interface-id</i>	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:

```
Switch# configure terminal
Switchconfig) 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

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.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source
```

This example shows how to enable IP source guard with MAC address verification:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# ip verify source mac-check
```

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 10
Switch(config-if)# switchport trunk allowed vlan 11-20
Switch(config-if)# no ip dhcp snooping trust
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config)# end
Switch# show ip verify source interface fastethernet0/1
```

Interface	Filter-type	Filter-mode	IP-address	Mac-address	Vlan
-----	-----	-----	-----	-----	-----
Gil/0/1	ip-mac	active	10.0.0.1		10
Gil/0/1	ip-mac	active	deny-all		11-20

Switch#

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface gigabitethernet1/0/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

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, see [device-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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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	<i>maximum</i> 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:

```
Switch(config)# ipv6 nd inspection policy policy1
Switch(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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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:	
	<pre>Switch(config)# mab request format attribute 32 vlan access-vlan</pre>	

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.

Command	Description
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 {namenum} [{namenum}] [{namenum}] . . .|ipv6 address {namenum}
[{namenum}] [{namenum}] . . .|mac address {name} [{name}] [{name}] . . .}
no match {ip address {namenum} [{namenum}] [{namenum}] . . .|ipv6 address
{namenum} [{namenum}] [{namenum}] . . .|mac address {name} [{name}] [{name}] . . .}
```

Syntax Description	
ip address	Sets the access map to match packets against an IP address access list.
ipv6 address	Sets the access map to match packets against an IPv6 address access list.
mac address	Sets the access map to match packets against a MAC address access list.
<i>name</i>	Name of the access list to match packets against.
<i>number</i>	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, IPv6 packets are matched against IPv6 access lists, and all other packets are matched against MAC access lists.

IP, IPv6, 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:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
```

```
Switch(config-access-map)# exit  
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

Related Topics

- [action](#), on page 765
- [show vlan access-map](#), on page 856
- [vlan access-map](#), on page 887

authentication logging verbose

To filter detailed information from authentication system messages, use the **authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

authentication logging verbose
no authentication logging verbose

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

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:

```
Switch(config)# authentication logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

```
dot1x logging verbose
no dot1x logging verbose
```

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

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:

```
Switch(config)# dot1x logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands	Command	Description
	authentication logging verbose	Filters details from authentication system messages.
	dot1x logging verbose	Filters details from 802.1x system messages.
	mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

mab logging verbose
no mab logging verbose

Syntax Description This command has no arguments or keywords.

Command Default Detailed logging of system messages is not enabled.

Command Modes Global configuration (config)

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:

```
Switch(config)# mab logging verbose
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

Related Commands

Command	Description
authentication logging verbose	Filters details from authentication system messages.
dot1x logging verbose	Filters details from 802.1x system messages.
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 | hostsrc-MAC-addr | src-MAC-addr mask} {any | hostdst-MAC-addr |
dst-MAC-addr mask} [type mask | aarp | amber | appletalk | dec-spanning | decnet-iv |
diagnostic | dsm | etype-6000 | etype-8042 | lat | larc-sca | lsap/sap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
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 | larc-sca | lsap lsap mask | mop-console
| mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [coscos]
```

Syntax Description

any	Denies any source or destination MAC address.
host <i>src-MAC-addr</i> <i>src-MAC-addr mask</i>	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 <i>dst-MAC-addr</i> <i>dst-MAC-addr mask</i>	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.
<i>type mask</i>	(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet. <ul style="list-style-type: none"> <i>type</i> is 0 to 65535, specified in hexadecimal. <i>mask</i> 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.
lavr-sca	(Optional) Specifies EtherType DEC-LAVC-SCA.
lsap <i>lsap-number mask</i>	(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. The <i>mask</i> 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 <i>cos</i>	(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.

```
Switch(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:

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Switch(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.

Command	Description
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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
```

radius server



Note Starting from Cisco IOS 15.2(5)E release, the **radius server** command replaces the **radius-server host** command, being used in releases prior to Cisco IOS Release 15.2(5)E. The old command has been deprecated.

Use the **radius server** configuration sub-mode command on the switch stack or on a standalone switch to configure the RADIUS server parameters, including the RADIUS accounting and authentication. Use the **no** form of this command to return to the default settings.

```
radius server name
address {ipv4 | ipv6} ip{address | hostname} auth-port udp-port acct-port udp-port
key string
automate tester name | retransmit value | timeout seconds
no radius server name
```

Syntax Description

address { ipv4 ipv6 } <i>ip{address hostname}</i>	Specify the IP address of the RADIUS server.
auth-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS authentication server. The range is from 0 to 65536.
acct-port <i>udp-port</i>	(Optional) Specify the UDP port for the RADIUS accounting server. The range is from 0 to 65536.
key <i>string</i>	(Optional) Specify the authentication and encryption key for all RADIUS communication between the switch and the RADIUS daemon. Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in this command. Leading spaces are ignored, but spaces within and at the end of the key are used. If there are spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.
automate tester <i>name</i>	(Optional) Enable automatic server testing of the RADIUS server status, and specify the username to be used.
retransmit <i>value</i>	(Optional) Specifies the number of times a RADIUS request is resent when the server is not responding or responding slowly. The range is 1 to 100. This setting overrides the radius-server retransmit global configuration command setting.
timeout <i>seconds</i>	(Optional) Specifies the time interval that the Switch waits for the RADIUS server to reply before sending a request again. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting.
no radius server <i>name</i>	Returns to the default settings

Command Default

- The UDP port for the RADIUS accounting server is 1646.
- The UDP port for the RADIUS authentication server is 1645.
- Automatic server testing is disabled.
- The timeout is 60 minutes (1 hour).
- When the automatic testing is enabled, testing occurs on the accounting and authentication UDP ports.
- The authentication and encryption key (string) is not configured.

Command Modes

Radius server sub-mode configuration

Command History

Release	Modification
Cisco IOS XE 3.2SE	This command was introduced to replace the radius-server host command.

Usage Guidelines

- We recommend that you configure the UDP port for the RADIUS accounting server and the UDP port for the RADIUS authentication server to non-default values.
- You can configure the authentication and encryption key by using the **key string** sub-mode configuration command. Always configure the key as the last item in this command.
- Use the **automate-tester name** keywords to enable automatic server testing of the RADIUS server status and to specify the username to be used.

This example shows how to configure 1645 as the UDP port for the authentication server and 1646 as the UDP port for the accounting server, and configure a key string:

```
Switch(config)# radius server ISE
Switch(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Switch(config-radius-server)# key cisco123
```

router rip

To configure the Routing Information Protocol (RIP) routing process, use the **route r rip** command in global configuration mode. To turn off the RIP routing process, use the **no** form of this command.

router rip
no router rip

Syntax Description This command has no arguments or keywords.

Command Default No RIP routing process is defined.

Command Modes
 Global configuration (config)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E2	This command was introduced.

Examples The following example shows how to begin the RIP routing process:

```
Device(config)# router rip
```

Related Commands	Command	Description
	network (RIP)	Specifies a list of networks for the RIP process.

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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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	<i>ip-address</i> 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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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:

```
Switch# 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:

```
Switch# show aaa command handler

AAA Command Handler Statistics:
account-logon: 0, account-logout: 0
account-query: 0, pod: 0
service-logon: 0, service-logout: 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.
	<i>name</i>	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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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

Cisco IOS XE 3.2SE

Modification

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:

```
Switch# 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 <i>handle-id</i>	(Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
details	(Optional) Shows detailed information.
interface <i>type number</i>	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
mac <i>mac-address</i>	(Optional) Specifies the particular MAC address for which you want to display information.
method <i>method-name</i>	(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 <i>session-id</i>	(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.

State	Description
Success	The method has provided a successful authentication result for the session.
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:

```
Switch# 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:

```
Switch# 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: 0A3462C80000000000002763C
      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 auto security

To display auto security status, use the **show auto security** command in privileged EXEC mode.

show auto-security

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.2(5)E	This command was introduced in a release prior to Cisco IOS Release 15.2(5)E.

Usage Guidelines

Configuring the **auto security** command in global configuration mode, configures auto security globally; including all interfaces. When you disable auto security, it is disabled on all interfaces.

Use the **auto security-port** command to enable auto security on specific interfaces.

The following is sample output from the **show auto security** command, when auto security is enabled globally:

```
Switch# show auto security

Auto Security is Enabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
GigabitEthernet1/0/3
GigabitEthernet1/0/4
GigabitEthernet1/0/5
GigabitEthernet1/0/7
GigabitEthernet1/0/8
GigabitEthernet1/0/10
GigabitEthernet1/0/12
GigabitEthernet1/0/23
```

The following is sample output from the **show auto security** command, when auto security is enabled on a specific interface:

```
Switch# show auto security

Auto Security is Disabled globally

AutoSecurity is Enabled on below interface(s):
-----
GigabitEthernet1/0/2
```

Related Commands

Command	Description
auto security	Configures global auto security.
auto security-port	Configures auto security on an interface.

show cisp

To display CISP information for a specified interface, use the **show cisp** command in privileged EXEC mode.

show cisp {[**clients** | **interface** *interface-id*] | **registrations** | **summary**}

Syntax Description		
clients		(Optional) Display CISP client details.
interface <i>interface-id</i>		(Optional) Display CISP information about the specified interface. Valid interfaces include physical ports and port channels.
registrations		Displays CISP registrations.
summary		(Optional) Displays CISP summary.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.3.1	This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x and Cisco IOS XE Denali 16.2.x

This example shows output from the **show cisp interface** command:

```
Switch# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Switch# show cisp registrations
Interface(s) with CISP registered user(s):
-----
Fa1/0/13
Auth Mgr (Authenticator)
Gi2/0/1
Auth Mgr (Authenticator)
Gi2/0/2
Auth Mgr (Authenticator)
Gi2/0/3
Auth Mgr (Authenticator)
Gi2/0/5
Auth Mgr (Authenticator)
Gi2/0/9
Auth Mgr (Authenticator)
Gi2/0/11
Auth Mgr (Authenticator)
```

```
Gi2/0/13
Auth Mgr (Authenticator)
Gi3/0/3
Gi3/0/5
Gi3/0/23
```

Related Commands

Command	Description
cisp enable	Enable Client Information Signalling Protocol (CISP)
dot1x credentials <i>profile</i>	Configure a profile on a supplicant switch

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:

```
Switch# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

This is an example of output from the **show dot1x all count** command:

```
Switch# 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:

```
Switch# 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:

```
Switch> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch> 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:

```
Switch> 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.
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.

DHCP Snooping Statistic	Description
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.
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 ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database entries if relevant are routes being summarized based upon a summary address, use the **show ip rip database** command in privileged EXEC mode.

show ip rip database [*ip-address mask*]

Syntax Description	
<i>ip-address</i>	(Optional) Address about which routing information should be displayed.
<i>mask</i>	(Optional) Argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.

Command Default No default behavior or values.

Command Modes Privileged EXEC(#)

Command History	Release	Modification
	Cisco IOS Release 15.2(5)E2	This command was introduced.

Usage Guidelines Summary address entries will appear in the database only if relevant child routes are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

The RIP private database is populated only if triggered extensions to RIP are enabled with the **ip rip triggered** command.

Examples

The following output shows a summary address entry for route 10.11.0.0/16, with three child routes active:

```
Device# show ip rip database
10.0.0.0/8    auto-summary
10.0.0.0/8
    [1] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
192.168.0.0/8    auto-summary
192.168.0.0/8
    [2] via 172.16.0.10, 00:00:17, GigabitEthernet7/0/10
172.16.0.0/8    auto-summary
172.16.0.0/24    directly connected, GigabitEthernet7/0/10
```

The table below describes the fields in the display.

Table 30: show ip rip database Field Descriptions

Field	Description
10.0.0.0/8 auto-summary	Summary address entry.

Field	Description
172.16.0.0/24 directly connected, GigabitEthernet7/0/10	Directly connected entry for GigabitEthernet 7/0/10.

Related Commands

Commands	Description
debug ip rip	Displays information on RIP routing transactions.

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

Cisco IOS XE 3.2SE

Modification

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:

```
Switch# 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 31: 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".

Field	Description
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	
<i>interface-id</i>	(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.

```
Switch> 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.

```
Switch> 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 32: show storm-control Field Descriptions

Field	Description
Interface	Displays the ID of the interface.

Field	Description
Filter State	Displays the status of the filter: <ul style="list-style-type: none">• 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.
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.

Related Topics

[storm-control](#), on page 859

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	<i>map-name</i> (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:

```
Switch# show vlan access-map
Vlan access-map "vmap4" 10
  Match clauses:
    ip address: a12
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: a12
  Action:
    forward
```

Related Topics

- [show vlan filter](#), on page 857
- [vlan access-map](#), on page 887
- [vlan filter](#), on page 889

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 <i>name</i> (Optional) Displays filtering information for the specified VLAN access map.	
	vlan <i>vlan-id</i> (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:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

Related Topics

[show vlan access-map](#), on page 856

[vlan access-map](#), on page 887

[vlan filter](#), on page 889

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 <i>vlan-group-name</i> (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	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Release</th> <th style="text-align: left;">Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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:

```
Switch# show vlan group group-name group2 user_count
VLAN      : Count
-----
40         : 5
41         : 8
42         : 12
43         : 2
44         : 9
45         : 0
```

Related Topics

[vlan group](#), on page 890

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.
<i>level</i>	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.
<i>level-low</i>	(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.
<i>bps</i>	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.
<i>bps-low</i>	(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.
<i>pps</i>	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 (BPDU) 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:

```
Switch(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:

```
Switch(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:

```
Switch(config-if) # storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if) # storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

Related Topics

[show storm-control](#), on page 854

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 <i>time</i>	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:

```
Switch(config)# interface gigabitethernet1/0/1
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# no switchport port-security aging static
```

Related Topics

- [show interfaces switchport](#), on page 127
- [switchport port-security mac-address](#), on page 864
- [switchport port-security maximum](#), on page 867
- [switchport port-security violation](#), on page 869

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:

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(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:

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

Related Topics

[show interfaces switchport](#), on page 127

[switchport port-security aging](#), on page 862

[switchport port-security maximum](#), on page 867

[switchport port-security violation](#), on page 869

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}]]]
no switchport port-security maximum value [vlan [{vlan-list}]]]
```

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.

```
Switch(config)# interface gigabitethernet 2/0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

Related Topics

- [show interfaces switchport](#), on page 127
- [switchport port-security aging](#), on page 862
- [switchport port-security mac-address](#), on page 864
- [switchport port-security violation](#), on page 869

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:

```
Switch(config)# interface gigabitethernet2/0/2
Switch(config)# switchport port-security violation shutdown vlan
```

Related Topics

- [show interfaces switchport](#), on page 127
- [switchport port-security aging](#), on page 862
- [switchport port-security mac-address](#), on page 864
- [switchport port-security maximum](#), on page 867

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. <ul style="list-style-type: none"> 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.
<i>value</i>		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. <ul style="list-style-type: none"> 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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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:

```
Switch(config)# ipv6 nd inspection policy1
Switch(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:

```
Switch(config)# ipv6 snooping policy policy1
Switch(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

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 <i>retries</i>		(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 <i>milliseconds</i>		(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 <i>sec</i>		Configures EAP-broadcast key renew interval time in seconds (120 to 86400 seconds).
identity-request		Configures EAP ID request related parameters.
retries <i>retries</i>		(Optional) Specifies the maximum number of times (0 to 4 retries) that the controller request the EAP ID. The default value is 2.
timeout <i>seconds</i>		(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 <i>retries</i>	(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 <i>seconds</i>	(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** .

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 <i>mac-addr</i>	Specifies the provision list authorization settings.
	revert <i>number</i>	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 <i>key-size</i>	Specifies the device certificate key size settings.
	subject-params <i>country state city orgn dept email</i>	Specifies the device certificate settings. Country, state, city, organization, department, and email of the certificate authority.
	trustpoint <i>trustpoint</i>	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:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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	<i>index</i>	Specifies the IDS sensor internal index.
	ip-address <i>ip-addr</i> username <i>username</i> password <i>password_type password</i>	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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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
<p>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.</p> <p>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.</p>	<p>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.</p>

This example shows how to disable clients on the 802.11 association attempt after five consecutive failures.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 <i>mac-addr</i>		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 <i>mac-addr</i> <i>no-of-aps</i>		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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#wireless wps rogue 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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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.

```
Switch(config)# vlan access-map vac1  
Switch(config-access-map)# match ip address acl1  
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map `vac1`:

```
Switch(config)# no vlan access-map vac1
```

Related Topics

- [action](#), on page 765
- [match \(access-map configuration\)](#), on page 816
- [show vlan access-map](#), on page 856
- [vlan filter](#), on page 889

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

<i>mapname</i>	Name of the VLAN map entry.
vlan-list	Specifies which VLANs to apply the map to.
<i>list</i>	The list of one or more VLANs in the form <i>tt, uu-vv, xx, yy-zz</i> , 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:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry `map1` from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

Related Topics

- [show vlan access-map](#), on page 856
- [show vlan filter](#), on page 857
- [vlan access-map](#), on page 887

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

<i>group-name</i>	Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.
vlan-list <i>vlan-list</i>	Specifies one or more VLANs to be added to the VLAN group. The <i>vlan-list</i> 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:

```
Switch(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Switch(config)# no vlan group group1 vlan-list 7
```

Related Topics

[show vlan group](#), on page 858



PART **XI**

Stack Manager and High Availability

- [Stack Manager and High Availability, on page 893](#)



Stack Manager and High Availability

- [debug platform stack-manager](#), on page 894
- [main-cpu](#), on page 895
- [mode sso](#), on page 896
- [policy config-sync prc reload](#), on page 897
- [redundancy](#), on page 898
- [redundancy config-sync mismatched-commands](#), on page 899
- [redundancy force-switchover](#), on page 901
- [redundancy reload](#), on page 902
- [reload](#), on page 903
- [session](#), on page 905
- [set trace capwap ap ha](#), on page 906
- [set trace mobility ha](#), on page 907
- [set trace qos ap ha](#), on page 909
- [show checkpoint](#), on page 910
- [show etherchannel summary](#), on page 917
- [show platform ses](#), on page 918
- [show platform stack-manager](#), on page 924
- [show redundancy](#), on page 925
- [show redundancy config-sync](#), on page 929
- [show switch](#), on page 931
- [show trace messages capwap ap ha](#), on page 935
- [show trace messages mobility ha](#), on page 936
- [stack-mac persistent timer](#), on page 937
- [stack-mac update force](#), on page 939
- [standby console enable](#), on page 940
- [switch stack port](#), on page 941
- [switch priority](#), on page 943
- [switch provision](#), on page 944
- [switch renumber](#), on page 946

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 <i>switch-number</i>	(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 (config-red)
----------------------	---------------------------------------

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:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# standby console enable
Switch#
```

Related Topics

[standby console enable](#), on page 940

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:

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(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	<p>bulk Specifies bulk configuration mode.</p> <p>lbl Specifies line-by-line (lbl) configuration mode.</p>				
Command Default	The command is enabled by default.				
Command Modes	Redundancy configuration (config-red)				
Command History	<table border="1"> <thead> <tr> <th data-bbox="386 854 609 886">Release</th> <th data-bbox="609 854 954 886">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 898 609 974">Cisco IOS XE 3.2SE</td> <td data-bbox="609 898 954 974">This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch(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 (config)
----------------------	-------------------------------

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:

```
Switch(config)# redundancy
Switch(config-red)#
```

This example shows how to enter the main CPU submode:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(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:

```
Switch# redundancy config-sync validate mismatched-commands  
Switch#
```

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 go down.

If you use this command on a switch that is in a partial ring stack, the following warning message appears:

```
Switch# 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:

```
Switch# redundancy force-switchover
Switch#
```

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:

```
Switch# redundancy reload shelf
Switch#
```

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.
<i>LINE</i>	(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.
<i>stack-member-number</i>	(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.

Examples

This example shows how to reload the switch stack:

```
Switch# 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:

```
Switch# 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):

```
Switch# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

Related Topics

- [show switch](#), on page 931
- [switch priority](#), on page 943
- [switch renumber](#), on page 946

session

To access the diagnostic shell of a specific stack member or to access the Cisco IOS prompt of the standby Switch use the **session** command in privileged EXEC mode on the active Switch.

```
session {standby ios|switch [{stack-member-number}]}
```

Syntax Description	standby ios	Accesses the Cisco IOS prompt of the standby Switch.
	Note	You cannot configure the standby Switch 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 Switch, `-stby` is appended to the system prompt. You cannot configure the standby Switch at the `switch-stby>` prompt.

When you access the diagnostic shell of a stack member, `(diag)` is appended to the system prompt.

Examples

This example shows how to access stack member 3:

```
Switch# session switch 3
Switch(diag)>
```

This example shows how to access the standby Switch:

```
Switch# session standby ios
Switch-stby>
```

Related Topics

- [reload](#), on page 903
- [show switch](#), on page 931
- [switch priority](#), on page 943
- [switch renumber](#), on page 946

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]]}]|filteredswitchlevel {defaulttrace_level} [switch switch]}]}
```

Syntax Description	Parameter	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.
	<i>switch switch number</i>	Specifies the switch number.
	none	(Optional) Specifies the no filter option.
	switch switch	(Optional) Specifies the switch number.
	<i>filter name</i>	Trace adapted flag filter name.
	<i>filter_value</i>	(Optional) Value of the filter.
	switch switch	(Optional) Specifies the switch number.
	filtered	Specifies the filtered traces messages.
	<i>switch</i>	Specifies the switch number.
	level	Specifies the trace level.
	default	Specifies the unset trace level value.
	<i>trace_level</i>	Specifies the trace level.
	switch switch	(Optional) Specifies the switch 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:

```
Switch# 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 {defaulttrace_level} [switch
switch]{filteredswitch}}
```

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.
<i>WORD switch</i>	Specifies the switch.
<i>switch number</i>	Specifies the switch number. The value ranges from one to four.
none	Specifies no trace adapted flag filter.
switch switch	(Optional) Specifies the switch number.
<i>filter_name</i>	Trace adapted flag filter name.
<i>filter_value</i>	Trace adapted flag filter value.
switch switch	Specifies the switch number.
level	Specifies the trace level value.
default	Specifies the un-set trace level value.
<i>trace_level</i>	Specifies the trace level value.
switch switch	Specifies the switch number.
filtered	Specifies the filtered trace messages.
<i>switch</i>	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:

```
Switch# 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 {defaulttrace_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.
<i>filter_name</i>	(Optional)	Specifies the switch filter name.
<i>filter_value</i>	(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.
<i>trace_level</i>		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:

```
Switch# 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

```

show checkpoint

```

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

```

show checkpoint

```

-----
                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

```

show checkpoint

```
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_DHCPDN"
clientCallback @ 0xF4CA9D30
next = 0x91DF7728

clientID = 18
clientSeq = 18
clientName = "NG3K_SES_CLIENT_IPSG"
clientCallback @ 0xF4CED70
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 <i>stack-member-number</i>		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 929.
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.
<i>slave-name</i>	(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:

```
Switch# show redundancy
Redundant System Information :
```

show redundancy

```

-----
    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
Switch#

```

This example shows how to display redundancy facility client information:

```

Switch# 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:

```
Switch# 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

Switch#
```

This example shows how to display redundancy facility history information:

```
Switch# 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_APPFROGUE(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:

```
Switch# 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]
```

```
Switch#
```

This example shows how to display information about the redundancy facility state:

```
Switch# 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

Switch#
```

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:

```
Switch> show redundancy config-sync failures bem
BEM Failed Command List
-----

The list is Empty
```

This example shows how to display the MCL failures:

```
Switch> show redundancy config-sync failures mcl
Mismatched Command List
-----

The list is Empty
```

This example shows how to display the PRC failures:

```
Switch# 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	
<i>stack-member-number</i>	(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.

Examples

This example shows how to display summary stack information:

```
Switch# show switch
Switch/Stack Mac Address : 6400.f124.e900
```

Switch#	Role	Mac Address	Priority	H/W Version	Current 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:

```
Switch# show switch detail
Switch/Stack Mac Address : 2037.06ce.3f80 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current 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

Switch#	Stack Port Status		Neighbors	
	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:

```
Switch# 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:

```
Switch# show switch neighbors
Switch #      Port A      Port B
```

```

-----
      6      None      8
      8      6      None

```

This example shows how to display stack-port information:

```

Switch# 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.

```

Switch# show switch stack-ports summary
Switch#/  Stack  Neighbor  Cable  Link  Link  Sync  #  In
Port#     Port  Status    Length OK   Active OK  Changes  Loopback
          Status
-----
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 33: Show switch stack-ports summary Command Output

Field	Description
Switch#/Port#	Member number and its stack port number.
Stack Port Status	Status of the stack port. <ul style="list-style-type: none"> 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 <i>no cable</i> . 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 <i>link partner</i> is a stack port on a neighbor switch. <ul style="list-style-type: none"> 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.

Field	Description
Link Active	Whether a neighbor is connected on the other end of the stack cable. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.
# 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. <ul style="list-style-type: none"> • 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.

Related Topics

- [reload](#), on page 903
- [session](#), on page 905
- [stack-mac update force](#), on page 939
- [switch priority](#), on page 943
- [switch provision](#), on page 944
- [switch renumber](#), on page 946

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 <i>switch number</i>		Specifies the switch number. Value is one.
event	(Optional)	Displays wireless CAPWAP high availability events.
event <i>switch number</i>		Specifies the switch number. Value is one.
dump	(Optional)	Displays wireless CAPWAP high availability output.
dump <i>switch number</i>		Specifies the switch number. Value is one.
switch	(Optional)	Displays the switch number. The value is one.
switch <i>switch number</i>		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 display CAPWAP high availability output:

```
Switch# 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 <i>switch</i>		Specifies the switch number. Value is one.
detail	(Optional)	Displays wireless mobility HA details.
detail <i>switch</i>		Specifies the switch number. Value is one.
dump	(Optional)	Displays the wireless mobility HA output debugging.
dump <i>switch</i>		Specifies the switch number. Value is one.
switch <i>switch</i>	(Optional)	Displays the switch number.
switch <i>switch</i>		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 display wireless mobility high availability:

```
Switch# 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 [*{0time-value}*]
no stack-mac persistent timer

Syntax Description	<p>0 (Optional) Continues using the MAC address of the current active switch indefinitely, even after a new active switch takes over.</p> <p><i>time-value</i> (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.</p>				
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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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.

Examples

This example shows how to enable a persistent MAC address:

```
Switch(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.

Related Topics

[stack-mac update force](#), on page 939

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:

```
Switch> stack-mac update force
Switch>
```

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.

Related Topics

[show switch](#), on page 931

[stack-mac persistent timer](#), on page 937

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:

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# standby console enable
Switch(config-r-mc)#
```

Related Topics

[main-cpu](#), on page 895

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

<i>stack-member-number</i>	Current stack member number. The range is 1 to 9.
stack port <i>port-number</i>	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.
```

Examples

This example shows how to disable stack port 2 on member 4:

```
Switch# switch 4 stack port 2 disable
```

Related Topics

[show switch](#), on page 931

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.

Examples

This example shows how to change the priority value of stack member 6 to 8:

```
Switch# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

Related Topics

- [reload](#), on page 903
- [session](#), on page 905
- [show switch](#), on page 931
- [switch renumber](#), on page 946

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	<i>stack-member-number</i>	Stack member number. The range is 1 to 9.
	<i>type</i>	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.

Examples

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.

```
Switch(config)# switch 2 provision WS-xxxx
Switch(config)# end
```

```
Switch# 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:

```
Switch(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.

Related Topics

[show switch](#), on page 931

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.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
Switch# 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]
```

Related Topics

- [reload](#), on page 903
- [session](#), on page 905
- [show switch](#), on page 931
- [switch priority](#), on page 943



PART **XII**

System Management

- [System Management Commands, on page 949](#)



System Management Commands

- [arp](#), on page 952
- [boot](#), on page 953
- [cat](#), on page 954
- [clear location](#), on page 955
- [clear location statistics](#), on page 956
- [clear nmosp statistics](#), on page 957
- [clear wireless ccx statistics](#), on page 958
- [clear wireless client tsm dot11](#), on page 959
- [clear wireless location s69 statistics](#), on page 960
- [copy](#), on page 961
- [copy startup-config tftp:](#), on page 962
- [copy tftp: startup-config](#), on page 963
- [debug call-admission wireless all](#), on page 964
- [debug rfid](#), on page 965
- [debug voice diagnostics mac-address](#), on page 966
- [debug wps mfp](#), on page 967
- [delete](#), on page 968
- [dir](#), on page 969
- [emergency-install](#), on page 971
- [exit](#), on page 973
- [flash_init](#), on page 974
- [help](#), on page 975
- [license right-to-use](#), on page 976
- [location](#), on page 978
- [location algorithm](#), on page 982
- [location expiry](#), on page 983
- [location notify-threshold](#), on page 984
- [location plm calibrating](#), on page 985
- [location rfid](#), on page 986
- [location rssi-half-life](#), on page 987
- [mac address-table move update](#), on page 988
- [mgmt_init](#), on page 989
- [mkdir](#), on page 990

- more, on page 991
- nmsp notification interval, on page 992
- no debug all, on page 994
- rename, on page 995
- reset, on page 996
- rmdir, on page 997
- sdm prefer, on page 998
- set, on page 999
- show ap name config general, on page 1002
- show avc client, on page 1004
- show avc wlan, on page 1005
- show cable-diagnostics tdr, on page 1006
- show debug, on page 1008
- show env, on page 1009
- show flow monitor, on page 1012
- show license right-to-use, on page 1017
- show location, on page 1019
- show location ap-detect, on page 1020
- show mac address-table move update, on page 1022
- show nmsp, on page 1023
- show sdm prefer, on page 1024
- show tech-support wireless, on page 1026
- show wireless ap summary (MA), on page 1028
- show wireless ap summary, on page 1029
- show wireless band-select, on page 1030
- show wireless client calls, on page 1031
- show wireless client dot11, on page 1032
- show wireless client location-calibration, on page 1033
- show wireless client probing, on page 1034
- show wireless client summary, on page 1035
- show wireless client timers, on page 1036
- show wireless client voice diagnostics, on page 1037
- show wireless country, on page 1038
- show wireless detail, on page 1041
- show wireless dtls connections, on page 1042
- show wireless flow-control, on page 1043
- show wireless flow-control statistics, on page 1044
- show wireless load-balancing, on page 1045
- show wireless mobility summary, on page 1046
- show wireless performance, on page 1047
- show wireless pmk-cache, on page 1048
- show wireless probe, on page 1049
- show wireless sip preferred-call-no, on page 1050
- show wireless summary, on page 1051
- show wireless wlan summary, on page 1052
- show wlan name, on page 1053

- [shutdown](#), on page 1056
- [system env temperature threshold yellow](#), on page 1057
- [test cable-diagnostics tdr](#), on page 1059
- [traceroute mac](#), on page 1060
- [traceroute mac ip](#), on page 1063
- [trapflags](#), on page 1065
- [trapflags client](#), on page 1066
- [type](#), on page 1067
- [unset](#), on page 1068
- [version](#), on page 1070
- [wireless client](#), on page 1071
- [wireless client mac-address deauthenticate](#), on page 1073
- [wireless client mac-address](#), on page 1074
- [wireless load-balancing](#), on page 1079
- [wireless sip preferred-call-no](#), on page 1080

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	<i>ip_address</i> (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.
-------------------------	--

Examples	This example shows how to display the ARP table:
-----------------	--

```
Switch: 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
```

Related Topics

[set](#), on page 999

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.	
<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.	
<i>/file-url</i>	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 switch 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 switch using the *new-image.bin* image:

```
Switch: set BOOT flash:/new-images/new-image.bin
Switch: 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.

Examples

This example shows how to display the contents of an image file:

```
Switch: 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 <i>mac-address</i>	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:

```
Switch> 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:

```
Switch> 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):

```
Switch> 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:

```
Switch> 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.
	<i>client-mac-addr</i>	MAC address of the client.
	all	Specifies all access points.
	name <i>ap-name</i>	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:

```
Switch> 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:

```
Switch> 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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	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.

Examples

This example shows how to copy a file at the root:

```
Switch: 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.

Examples

This example shows how to copy the configuration settings onto a TFTP server:

```
Switch: 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	<i>remote host {ip-address}/{name}</i> 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.
-------------------------	---

Examples	This example shows how to copy the configuration settings from the TFTP server onto a switch:
-----------------	---

```
Switch: 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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

<i>debug_leaf_name</i>	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.
<i>filter</i>	Debug flag filter name.
switch <i>switch</i>	Configures RFID debugging for 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 rfid** command and shows how to enable debugging of RFID error messages:

```
Switch# 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**
no debug voice diagnostics mac-address *mac-address1* **verbose** **mac-address** *mac-address2* **verbose**

Syntax Description		
voice diagnostics		Configures voice debugging for voice clients.
mac-address <i>mac-address1</i> mac-address <i>mac-address2</i>		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:

```
Switch# 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	Option	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 <i>switch</i>	Displays the WPS MFP debugging for the 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.

This example shows how to enable WPS MFP debugging options for client:

```
Switch# 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 switch prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Switch: 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.

Examples

This example shows how to display the files in flash memory:

```
Switch: 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 34: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> • d—directory • r—readable • w—writable • x—executable

Field	Description
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Topics

[mkdir](#), on page 990

[rmdir](#), on page 997

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	<i><url></i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch: 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:

```
Switch(config)# exit
Switch#
```

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

Example

This example shows how to display a list of available boot loader commands:

```
Switch: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 switch, 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 <i>count</i>		Specifies the number of ap-count licenses added. You can configure the number of adder licenses from 5 to 50.
ipbase <i>count</i>		Activates ipbase licenses on the switch.
ipservices <i>count</i>		Activates ipservices licenses on the switch.
lanbase <i>count</i>		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:

```
Switch# license right-to-use activate apcount evaluation
Switch# end
```

This example shows how to activate an ap-count permanent license:

```
Switch# license right-to-use deactivate apcount evaluation
Switch# end
```

This example shows how to add a new ap-count license:

```
Switch# license right-to-use activate apcount 500 slot 1
Switch# 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 {hostid}|civic-location identifier
{hostid}|elin-location {string | identifier
id}|expiry{calibrating-clienttimeout-value | clienttimeout-value | rouge-aps timeout-value | tagsttimeout-value}|geo-location
identifier {hostid}|notify-threshold {clientdb | rouge-apsdb | tagsdb|plm {calibrating|{multiband
|uniband}|clientburst-interval}|prefer { cdp weightpriority-value | lldp-med weightpriority-value | static
config weightpriority-value} | rfid {status | timeout:rfid-timeout-value | vendor-namename} | rssi-half-life
{ calibrating-clientseconds | clientseconds | rouge-apsseconds | tagsseconds}
no location {admin-tag string|algorithm|civic-location identifier {hostid}|civic-location identifier
{hostid}|elin-location {string | identifier
id}|expiry{calibrating-clienttimeout-value | clienttimeout-value | rouge-aps timeout-value | tagsttimeout-value}|geo-location
identifier {hostid}|notify-threshold {clientdb | rouge-apsdb | tagsdb|plm {calibrating|{multiband
|uniband}|clientburst-interval}|prefer { cdp weightpriority-value | lldp-med weightpriority-value | static
config weightpriority-value} | rfid {status | timeout:rfid-timeout-value | vendor-namename} | rssi-half-life
{ calibrating-clientseconds | clientseconds | rouge-apsseconds | tagsseconds}
```

Syntax Description

admin-tag <i>string</i>	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.
<i>id</i>	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 } <i>timeout-value</i>	Configures the timeout for RSSI values for calibrating clients, clients, rogue 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 } <i>db</i>	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 <i>seconds</i>	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.
rfd	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:

```
Switch(config)# location civic-location identifier 1
Switch(config-civic)# number 3550
Switch(config-civic)# primary-road-name "Cisco Way"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state CA
Switch(config-civic)# building 19
Switch(config-civic)# room C6
Switch(config-civic)# county "Santa Clara"
Switch(config-civic)# country US
Switch(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:

```
Switch(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:

```
Switch(config)# location geo-location identifier host
Switch(config-geo)# latitude 12.34
Switch(config-geo)# longitude 37.23
Switch(config-geo)# altitude 5 floor
Switch(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:

```
Switch# configure terminal
Switch(config)# location algorithm rssi-average
Switch(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.
<i>timeout-value</i>	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:

```
Switch# configure terminal
Switch(config)# location expiry client 1000
Switch(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.
<i>db</i>	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:

```
Switch# configure terminal
Switch(config)# location notify-threshold client 10
Switch(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	uniband
	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.	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:

```
Switch# configure terminal
Switch(config)# location plm calibrating uniband
Switch(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:

```
Switch# configure terminal
Switch(config)# location rfid timeout 1000
Switch(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.
<i>seconds</i>	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:

```
Switch# configure terminal
Switch(config)# location rssi-half-life client 100
Switch(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					
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# configure terminal
Switch(config)# mac address-table move update transmit
Switch(config)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Switch# configure terminal
Switch(config)# mac address-table move update receive
Switch(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.

Examples This example shows how to initialize the Ethernet management port:

```
Switch: 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	<i>filesystem:</i> Alias for a file system. Use usbflash0: for USB memory sticks.
	<i>/directory-url...</i> 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	<p>Directory names are case sensitive.</p> <p>Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.</p>
-------------------------	---

Example

This example shows how to make a directory called Saved_Configs:

```
Switch: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

Related Topics

[dir](#), on page 969

[rmdir](#), on page 997

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.

Examples

This example shows how to display the contents of a file:

```
Switch: 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:

```
Switch# configure terminal
Switch(config)# nmsp notification-interval rfid 25
Switch(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:

```
Switch# configure terminal
Switch(config)# nmsp notification-interval attachment 10
Switch(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Switch# configure terminal  
Switch(config)# nmsp notification-interval location 20  
Switch(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.

Examples

This example shows how to disable debugging on a switch.

```
Switch: 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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/source-file-url</i>	Original path (directory) and filename.
<i>/destination-file-url</i>	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.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
Switch: 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 switch; 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.

Examples

This example shows how to reset the system:

```
Switch: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

Related Topics

[reset](#), on page 996

[test cable-diagnostics tdr](#), on page 1059

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 switch prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Switch: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

Related Topics

[dir](#), on page 969

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	<p>In a switch stack, all stack members must use the same SDM template that is stored on the active switch.</p> <p>When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.</p>
-------------------------	--

Example

This example shows how to configure the advanced template:

```
Switch(config)# sdm prefer advanced
Switch(config)# exit
Switch# reload
```

Related Topics

[show sdm prefer](#), on page 1024

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 switch.

set *variable value*

Syntax Description

<i>variable</i> <i>value</i>	<p>Use one of the following keywords for <i>variable</i> and the appropriate value for <i>value</i>:</p> <p>MANUAL_BOOT—Decides whether the switch automatically or manually boots.</p> <p>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 switch from the boot loader mode.</p>
	<p>BOOT filesystem:/file-url—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting.</p> <p>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.</p>
	<p>ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the Break key on the console.</p> <p>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.</p>
	<p>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.</p>
	<p>PS1 prompt—Specifies a string that is used as the command-line prompt in boot loader mode.</p>
	<p>CONFIG_FILE flash: /file-url—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p>
	<p>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.</p> <p>The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</p>
	<p>SWITCH_NUMBER stack-member-number—Changes the member number of a stack member.</p>
	<p>SWITCH_PRIORITY priority-number—Changes the priority value of a stack member.</p>

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 switch:

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 switch *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:

```
Switch: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

Related Topics

[reset](#), on page 996

[unset](#), on page 1068

show ap name config general

To display detailed information of an MA access point, use the **show ap name config general** command.

show ap name *ap-name* *ma-ip* config general

Syntax Description	<i>ap-name</i>	Access Point name.
	<i>ma-ip</i>	MA IPv4 Address.
Command Default	None	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.
Usage Guidelines	This command works only with MC.	

Example

The following example shows how to display the detailed information of an MA access point:

```
Cisco controller# show ap name AP5 211.0.0.4 config general

Cisco AP Name                : AP5
Cisco AP Identifier          : 0
Country Code                 : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A      802.11a:-AB
AP Country Code              : US - United States
AP Regulatory Domain
  Slot 0                     : -A
  Slot 1                     : -A
Switch Port Number           : Gi1/0/5
MAC Address                   : 6c20.56e1.4a57
IP Address Configuration     : DHCP
IP Address                   : 211.0.0.170
IP Netmask                    : 255.255.255.0
Gateway IP Address           : 211.0.0.100
CAPWAP Path MTU              : 1485
Telnet State                  : Disabled
SSH State                     : Disabled
Jumbo MTU Status             : Disabled
Cisco AP Location            : default location
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              : 10.3.123.92
Boot Version                  : 12.4.23.0
Stats Reporting Period        : 180
LED State                     : Enabled
PoE Pre-Standard Switch      : Disabled
```

```
PoE Power Injector MAC Address      : Disabled
Power Type/Mode                     : PoE/Full Power (normal mode)
Number of Slots                     : 2
AP Model                             : AIR-CAP3602I-A-K9
AP Image                             : C3600-K9W8-M
IOS Version                          : 15.3(20151222:165605)$
Reset Button                         : Enabled
AP Serial Number                    : FGL1645W0W1
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                           : 23 minutes 53 seconds
AP CAPWAP Up Time                   : 21 minutes 53 seconds
Join Date and Time                   : 01/18/2016 02:36:09
Join Taken Time                      : 1 minute 59 seconds
Ethernet Port Duplex                 : Auto
Ethernet Port Speed                  : Auto
AP Link Latency                      : Disabled
Rogue Detection                      : Enabled
AP TCP MSS Adjust                    : Disabled
AP TCP MSS Size                      : 0
AP IPv6 TCP MSS Adjust               : Disabled
AP IPv6 TCP MSS Size                 : 1220
```

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:

```
Switch# 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.3SE	This command was introduced.				

The following is sample output from the **show avc wlan** command:

```
Switch# 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	<i>interface-id</i> 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 switch:

```
Switch# 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 35: 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 switch. TDR can only find the location in one of these cases: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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:

```
Switch# 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:

```
Switch# 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 switch 1
```

Related Topics

[test cable-diagnostics tdr](#), on page 1059

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	<i>Condition identifier</i> Sets the value of the condition identifier to be used. Range is between 1 and 1000.
	<i>All conditions</i> 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.

Examples This example shows the output of a **show debug** command:

```
Switch# 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 <i>switch-number</i>		(Optional) Displays the power supply status for a specific switch.
stack <i>switch-number</i>		(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:

```
Switch> show env stack 1
Switch :1
Switch 1 Fan 1 is OK
Switch 1 Fan 2 is OK
```

```

Switch 1 Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>

```

This example shows how to display temperature value, state, and threshold values:

```

Switch> show env temperature status
Temperature Value: 26 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>

```

Examples

This example shows how to display information about stack member 1 from the master switch:

```

Switch> show env stack 1
Switch 1:
Switch Fan 1 is OK
Switch Fan 2 is OK
Switch Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Switch>

```

This example shows how to display temperature value, state, and threshold values:

```

Switch> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

```

Switch>

Table 36: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the <i>normal</i> operating range.
Yellow	The temperature is in the <i>warning</i> range. You should check the external temperature around the switch.
Red	The temperature is in the <i>critical</i> range. The switch might not run properly if the temperature is in this range.

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} | aggregate | filter | sort}]] [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.
<i>monitor-name</i>	(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.
aggregate	(Optional) Displays an aggregate of the given fields.
filter	(Optional) Filters and displays only matching flow records.
sort	(Optional) Sorts the resulting flow records in the required order.
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.

Examples

The following example displays the status for a flow monitor:

```
Switch# 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.
Status	Status of the flow monitor cache. The possible values are: <ul style="list-style-type: none"> • 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:

```
Switch# 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.
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.

Field	Description
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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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 licenses installed on the switch, 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	Option	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:

```
Switch# show license right-to-use usage
```

Slot#	License Name	Type	usage-duration (y:m:d)	In-Use	EULA
1	ipservices	Permanent	00:00:00	no	no
1	ipservices	Evaluation	00:00:00	no	no
1	ipbase	Permanent	01:11:12	yes	yes
1	ipbase	Evaluation	00:00:00	no	no
1	lanbase	Permanent	00:00:00	no	no

The following is sample output from the **show license right-to-use detail** command and displays the detailed information of licenses:

```
Switch# show license right-to-use detail

show license right-to-use detail
Index 1
```

```

License Name      : ipservices
Period left       : Lifetime
License Type      : Permanent
License State     : Not Activated
License Location  : Slot 1
Index 2
License Name      : ipservices
Period left       : 90
License Type      : Evaluation
License State     : Not Activated
License Location  : Slot 1
Index 3
License Name      : ipbase
Period left       : Lifetime
License Type      : Permanent
License State     : Active, In use
License Location  : Slot 1
Index 4
License Name      : ipbase
Period left       : 90
License Type      : Evaluation
License State     : Not Activated
License Location  : Slot 1
Index 5
License Name      : lanbase
Period left       : Lifetime
License Type      : Permanent
License State     : Not Activated
License Location  : Slot 1

```

The following is sample output from the **show license right-to-use summary** command when the evaluation license is active:

```
Switch# show license right-to-use summary
```

```

License Name      Type      Period left
-----
          ipbase Permanent      Lifetime
dna-advantage Subscription Subscription  Active
-----

```

```

License Level In Use: ipbase+dna-advantage Subscription
License Level on Reboot: ipbase+dna-advantage Subscription

```

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 <i>mac-addr</i>	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 <i>MAC-addr</i>	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:

```
Switch# 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.	
<i>ap-name</i>	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:

```
Switch# 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 switch, 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:

```
Switch# 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 nmosp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmosp** command.

```
show nmosp {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 nmosp notification interval** command:

```
Switch# show nmosp 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 switch 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:

```
Switch# 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.
```

Switch#

Related Topics

[sdm prefer](#), on page 998

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:

```
Switch# 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 ap summary (MA)

To display the wireless access point mobility agent (MA) summary information, use the **show wireless ap summary** command.

show wireless ap *ma-ip* summary

Syntax Description	<i>ma-ip</i>	MA IPv4 Address.
Command Default	None	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.
Usage Guidelines	This command works only with MC.	

Example

The following example shows how to display the wireless access point MA summary:

```
Cisco controller# show wireless ap 211.0.0.4 summary
```

```
Mobility Agent Access Point Summary:
```

```
Mobility Role                : Mobility Agent
Mobility Agent IP            : 211.0.0.4
Mobility Switch Peer Group Name : SPG1
Multicast Group IP Address   : 0.0.0.0
Capwap Multicast Iif-Id     : NA
Link Encryption              : Disabled
Total AP Joined              : 1
IOS Version                  : Not Available
AP software version          : 10.3.123.92
```

```
Codes U - Up, UR - Unregistered, D - Downloading, R - Registered
AP Up Time in hours:minutes:seconds
```

AP Name	AP Model	Port	IP Address	Radio(Ghz)	State	Radio MAC	AP
UpTime	Clients						
AP5	3602I	Gi1/0/5	211.0.0.170	2.4, 5	R	1ce6.c75b.3e70	
00:21:06	0						

show wireless ap summary

To display the number of access points known to the controller, use the **show wireless ap summary** command.

show wireless ap summary

Syntax Description	This command has no keywords or arguments	
Command Default	None	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.

The following example shows how to display the number of access points known to the controller:

```
Cisco controller# show wireless ap summary
```

```
Sub-Domain Access Point Summary
```

```
Maximum AP Limit: 100
Total AP License Installed: 60
Total AP License Available: 59
Total AP Joined: 1
```

```
AP UpTime in hours:minutes:seconds
```

HostName	Controller IP	AP name	AP Group	AP Model	AP IP
AP UpTime	Clients				
Switch	52.2.2.1	APd48c.b5e1.05bd	default-group	1142N	52.2.2.155
452:37:01	0				

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:

```
Switch# 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 switch, 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:

```
switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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).

```
Switch# 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:

```
Switch# 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	Parameter	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:

```
Switch# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```


The following is sample output from the **show wireless country configured** command:

```
Switch# show wireless country configured
Configured Country.....: US - United States
Configured Country Codes
  US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g
```

The following is sample output from the **show wireless country supported tx-power** command:

```
Switch# show wireless country supported tx-power
KEY: ##      = Tx Power in dBm.
     ##*     = Channel supports radar detection .
     .       = Channel is not legal in this country.
     (-)     = Regulatory Domains allowed by this country.
     (-,-)   = (indoor, outdoor) regulatory Domains 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
-----:+++++-----:
(-CE , -CE ) AE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) AL  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AR ) AR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) AT  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -NA ) AU  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) BA  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) BE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) BG  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -   ) BH  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -A  ) BO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -AR ) BR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) BY  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -ABN) CA  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -ABN) CA2 : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) CH  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AER , -AR ) CL  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) CM  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-CE  , -CE ) CN  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AR ) CO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-A  , -AB  ) CR  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) CY  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) CZ  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) DE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) DK  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -ABN) DO  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -   ) DZ  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A  , -AB  ) EC  : 27 27 27 27 27 27 27 27 27 27 27 27 27 27 .
(-E  , -E  ) EE  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) EG  : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E  , -E  ) ES  : 20 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 20 .
(-E  , -E  ) FR  : 20 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 20 .
(-E  , -E  ) GI  : 20 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 20 .
(-A  , -NA ) HK  : 27 27 27 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 20 .
(-E  , -E  ) HU  : 20 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 20 .
(-E  , -E  ) IE  : 20 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 20 .
```

show wireless country

```

(-I , -I ) ILO : . . . . 20 20 20 20 20 20 20 20 20 20 .
(-A , -AN ) IN : 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 .
(-E , -E ) IS : 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 .
(-JPU , -JPU ) J2 : 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
(-JPQU , -PQ ) J4 : 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 .
(-JPU , -JPU ) JP : 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 .
(-E , -E ) KN : 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 .
(-E , -E ) KW : 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 .
(-E , -E ) LB : 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 .
(-E , ) LK : 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 .
(-E , -E ) LU : 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 .
(-E , -E ) MC : 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 .
(-E , -E ) MK : 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 .
(-E , -E ) MT : 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 .
(-E , -E ) NL : 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 .
(-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 .
(-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 .
(-E , -E ) PL : 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 .
(-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 .
(-E , -E ) RO : 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 .
(-AER , -ER ) RU : 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 .
(-E , -E ) SE : 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
(-E , -E ) SI : 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 .
(-E , -ER ) TH : 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 .
(-EI , -E ) TR : 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 .
(-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 .
(-E , -E ) ZA : 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:

```
Switch# 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:

```
Switch# 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	<i>channel-id</i> Identification number for a channel through which flow control is monitored.				
Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.3SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
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:

```
Switch# 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	<i>channel-id</i> 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:

```
Switch# 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 mobility summary

To display the summary of the mobility management configuration, use the **show wireless mobility summary** command.

show wireless mobility *ma-ip* summary

Syntax Description	<i>ma-ip</i>	MA IPv4 Address.
Command Default	None	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.
Usage Guidelines	This command works only with MC.	

Example

The following example shows how to display the summary of the mobility management configuration:

```
Cisco controller# show wireless mobility 211.0.0.4 summary
```

```
Mobility Agent Summary:
```

```
Mobility Role                : Mobility Agent
Wireless Management VLAN     : 211
Wireless Management IP Address : 211.0.0.4
Mobility Switch Peer Group Name : SPG1
Multicast IP Address         : 0.0.0.0
DTLS Mode                    : Enabled
Mobility Keepalive Interval/Count : 10/3
Mobility Control Message DSCP Value : 48
Switch Peer Group Members Configured : 1
Central Management           : Enabled
```

```
Link Status is Control Link Status : Data Link Status
```

```
The status of Mobility Controller:
```

```
Host Name      IP          Public IP      Link Status
-----
ct3850-62     211.0.0.8    211.0.0.8     UP   : UP
```

```
Switch Peer Group members:
```

```
Host Name      IP          Public IP      Data Link Status
-----
ct3850-63     211.0.0.4    211.0.0.4     N/A
```

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.

```
Switch# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Switch# 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 <i>mac-addr</i> (Optional) Information about a single entry in the PMK cache.				
Command Default	No default behavior or values.				
Command Modes	Privileged EXEC				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# 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
```

show wireless wlan summary

To display wireless WLAN details, 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
	Cisco IOS XE 3.7.3E	This command was introduced.

The following example shows how to display wireless WLAN summary:

```
Cisco controller# show wireless WLAN summary
```

```
Total WLAN Configured: 2
```

```
Total Client Count: 0
```

ID	Profile Name Status	SSID	Security	Radio	VLAN	Client
1	benimr3 UP	benimr3	NONE	All	602	0
2	Proton_2 UP	Proton_2	NONE	All	202	0

show wlan name

To display the MA's WLAN configuration by name, use the **show wlan name** command.

show wlan name *name ma-ip*

Syntax Description	<i>name</i>	Access point name.
	<i>ma-ip</i>	MA IPv4 address.
Command Default	None	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.
Usage Guidelines	This command works only with MC.	

Example

The following example shows how to display the MA WLAN configuration by name:

```
Cisco controller# show wlan name anu_mcma 211.0.0.4

WLAN Profile Name      : anu_mcma
=====
Identifier              : 1
Network Name (SSID)    : anu_mcma
Status                  : Disabled
Broadcast SSID         : Enabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 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              : 211
Interface Status       : Up
Multicast Interface    : Unconfigured
WLAN IPv4 ACL          :
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
Local Profiling -Policy Name : Disabled
Device Classification  : Disabled
QoS Service Policy - Input
```

show wlan name

```

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
WMM : Allowed
WifiDirect : 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 : MACFILTER
Accounting list name : Disabled
802.1x authentication list name : wcm_dot1x
Security
802.11 Authentication : Open System
Static WEP Keys : Disabled
802.1X : Disabled
Wi-Fi Protected Access (WPA/WPA2)
WPA (SSN IE) : Disabled
WPA2 (RSN IE) : Enabled
TKIP Cipher : Disabled
AES Cipher : Enabled
Auth Key Management
802.1x : Enabled
PSK : Disabled
CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
PMF dot1x : Disabled
PMF PSK : Disabled
FT Support : Disabled
FT Reassociation Timeout : 20
FT Over-The-DS mode : Enabled
PMF Support : Disabled
PMF Association Comeback Timeout : 1
PMF SA Query Time : 200
CKIP : Disabled
IP Security : 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
Local HTTP Profiling Status : Disabled
Radius HTTP Profiling Status : Disabled
Assisted-Roaming
  Neighbor List : Disabled
  Prediction List : Disabled
  Dual Band Support : Disabled
AVC Visibility : Disabled
Universal Ap Admin : Disabled
llac Mu Mimo : Disabled
```

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 <i>vlan-id</i>	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:

```
Switch(config)# vlan open1
Switch(config-wlan)# shutdown
```

This example shows that the access point is not shut down:

```
Switch# configure terminal
Switch(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

Switch	Difference between Yellow and Red	Red ¹³
Catalyst 3850	14°C	60°C

¹³ 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 9 by using the **system env temperature threshold yellow 9** command.



Note

The internal temperature sensor in the switch measures the internal system temperature and might vary ± 5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Switch(config)# system env temperature threshold yellow 15
Switch(config)#
```

■ system env temperature threshold yellow

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	<i>interface-id</i> 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:

```
Switch# 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 a link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Switch# 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.
```

Related Topics

[show cable-diagnostics tdr](#), on page 1006

tracert 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 **tracert mac** command in privileged EXEC mode.

```
tracert mac [interface interface-id] source-mac-address [interface interface-id]
destination-mac-address [vlan vlan-id] [detail]
```

Syntax Description

interface <i>interface-id</i>	(Optional) Specifies an interface on the source or destination switch.
<i>source-mac-address</i>	The MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination switch in hexadecimal format.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. 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 tracert to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 tracert, the switch 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 tracert 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 **tracert 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 tracert 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:

```
Switch# 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:

```
Switch# 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 switches:

```
Switch# 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 switch is not connected to the source switch:

```
Switch# 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 switch cannot find the destination port for the source MAC address:

```
Switch# tracert 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:

```
Switch# tracert 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:

```
Switch# tracert mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# tracert mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Topics

[tracert mac ip](#), on page 1063

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		
<i>source-ip-address</i>	The IP address of the source switch as a 32-bit quantity in dotted-decimal format.	
<i>source-hostname</i>	The IP hostname of the source switch.	
<i>destination-ip-address</i>	The IP address of the destination switch as a 32-bit quantity in dotted-decimal format.	
<i>destination-hostname</i>	The IP hostname of the destination switch.	
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 switch in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch 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 switch 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 switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch 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:

```
Switch# tracroute 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:

```
Switch# tracroute 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:

```
Switch# tracroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Topics

[tracroute mac](#), on page 1060

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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# configure terminal
Switch(config)# no trapflags rogueap
Switch(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:

```
Switch# configure terminal
Switch(config)# trapflags client dot11 disassociate
Switch(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	<i>filesystem:</i> Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
---------------------------	---

<i>/file-url...</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

Usage Guidelines	<p>Filenames and directory names are case sensitive.</p> <p>If you specify a list of files, the contents of each file appear sequentially.</p>
-------------------------	--

Examples	<p>This example shows how to display the contents of a file:</p>
-----------------	--

```
Switch: 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 switch 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:

```
Switch: unset SWITCH_PRIORITY
```

Related Topics

[set](#), on page 999

[reset](#), on page 996

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.

Examples

This example shows how to display the boot loader version on a switch:

```
Switch: 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}
```

Syntax Description

association limit <i>assoc-number</i> interval <i>interval</i>	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 the band select options for the client.
client-rssi <i>rssi</i>	Sets the client received signal strength indicator (RSSI) threshold for band select. The minimum dBm of a client RSSI to respond to probe is between -90 and -20.
cycle-count <i>count</i>	Sets the band select probe cycle count. You can configure the cycle count from 1 to 10.
cycle-threshold <i>threshold</i>	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from 1 to 1000 milliseconds.
expire dual-band <i>timeout</i>	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 to 300 seconds, and the default value is 60 seconds.
expire suppression <i>timeout</i>	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 to 200 seconds, and the default timeout value is 20 seconds.
max-user-login <i>max-user-login</i>	Configures the maximum number of login sessions for a user.
timers auth-timeout <i>seconds</i>	Configures the client timers.

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 probe cycle count for band select to 8:

```
Switch# configure terminal  
Switch(config)# wireless client band-select cycle-count 8  
Switch(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Switch# configure terminal  
Switch(config)# wireless client band-select cycle-threshold 700  
Switch(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Switch# configure terminal  
Switch(config)# wireless client band-select expire suppression 70  
Switch(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 <i>mac-addr</i> Wireless client MAC address.				
Command Default	No default behavior or values.				
Command Modes	Global configuration				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to disconnect a wireless client:

```
Switch# configure terminal
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Switch(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 {anyprofile-id}}
```

Syntax Description

<i>mac-addr</i>	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 <i>hostname</i> <i>host-name</i>	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 <i>measurement-duration</i>	Sends 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 <i>ssid bssid</i> <i>dot11 channel</i>	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.
<i>profile-id</i>	(Optional) Test profile name.
<i>bssid</i>	Basic SSID.
<i>dot11</i>	Specifies the 802.11a, 802.11b, or 802.11g network.
<i>channel</i>	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.
<i>profile-id</i>	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:

```
Switch# configure terminal
```

```
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Switch(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 <i>denial-count</i>	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 <i>client-count</i>	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:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial 5
Switch(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:

```
Switch# configure terminal
Switch(config)# wireless sip preferred-call-no 2 0123456789
Switch(config)# end
```



PART **XIII**

VideoStream

- [VideoStream Commands](#), on page 1083



VideoStream Commands

- [ap dot11 media-stream multicast-direct](#), on page 1084
- [show ap dot11](#), on page 1085
- [show wireless media-stream group](#), on page 1086
- [wireless media-stream multicast-direct](#), on page 1087
- [wireless media-stream](#), on page 1088

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 <i>value</i>	Specifies the maximum number of streams allowed on a client.
radio-maximum <i>value</i>	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) >Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#ap dot11 24ghz media-stream multicast-direct
```

Related Topics

[wireless media-stream multicast-direct](#), on page 1087

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.

```
Switch#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
```

Related Topics

[wireless media-stream](#), on page 1088

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 <i>groupName</i>	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.

Related Topics

[wireless media-stream](#), on page 1088

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.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(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 <i>groupName</i>	Configure multicast-direct status for a group.	
<i>startipAddr</i>	Specifies the start IP Address for the group.	
<i>endipAddr</i>	Specifies the End IP Address for the group.	
group <i>avg-packet-size</i>	Configure average packet size.	
group <i>default</i>	Set a command to its defaults.	
group <i>exit</i>	Exit sub-mode.	
group <i>max-bandwidth</i>	Configure maximum expected stream bandwidth in Kbps.	
group <i>no</i>	Negate a command or set its defaults.	
group <i>policy</i>	Configure media stream admission policy.	
group <i>qos</i>	Configure over the air QoS class, <'video'> ONLY.	
multicast-direct	Configure multicast-direct status.	
message	Configure Session Announcement Message.	
phone <i>phone</i>	Configure Session Announcement Phone number.	
URL <i>URL</i>	Configure Session Announcement URL.	
Notes <i>Notes</i>	Configure Session Announcement notes.	
Email <i>Email</i>	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.

```
Switch#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Switch(config)#wireless media-stream group GROUP1 231.1.1.1 231.1.1.10
```




PART **XIV**

VLAN

- [VLAN, on page 1093](#)



VLAN

- [client vlan, on page 1094](#)
- [clear vtp counters, on page 1095](#)
- [debug platform vlan, on page 1096](#)
- [debug sw-vlan, on page 1097](#)
- [debug sw-vlan ifs, on page 1099](#)
- [debug sw-vlan notification, on page 1100](#)
- [debug sw-vlan vtp, on page 1102](#)
- [interface vlan, on page 1104](#)
- [show platform vlan, on page 1106](#)
- [show vlan, on page 1107](#)
- [show vtp, on page 1110](#)
- [show wireless vlan group, on page 1116](#)
- [switchport priority extend, on page 1117](#)
- [switchport trunk, on page 1118](#)
- [vlan, on page 1121](#)
- [vlan dot1q tag native, on page 1127](#)
- [vtp \(global configuration\), on page 1128](#)
- [vtp \(interface configuration\), on page 1133](#)
- [vtp primary, on page 1134](#)
- [wireless broadcast vlan, on page 1135](#)

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	<i>interface-id-name-or-group-name</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.

Related Topics

[show vtp](#), on page 1110

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 <i>switch-number</i>	(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:

```
Switch# 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 1099 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 1100 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 1102 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:

```
Switch# debug sw-vlan events
```

Related Topics

- [debug sw-vlan ifs](#), on page 1099
- [debug sw-vlan notification](#), on page 1100
- [debug sw-vlan vtp](#), on page 1102
- [show vlan](#), on page 1107
- [show vtp](#), on page 1110

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:

```
Switch# debug sw-vlan ifs write
```

Related Topics

[show vlan](#), on page 1107

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:

```
Switch# debug sw-vlan notification
```

Related Topics

[show vlan](#), on page 1107

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 **undebg 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:

```
Switch# debug sw-vlan vtp redundancy
```

Related Topics

[show vtp](#), on page 1110

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:

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

Related Topics

[show interfaces](#), on page 121

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		
<i>vlan-id</i>	(Optional) ID of the VLAN. The range is 1 to 4094.	
switch <i>switch-number</i>	(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:

```
Switch# 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 <i>vlan-id</i>	(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <i>vlan-id</i> , 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 <i>vlan-name</i>	(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.

```
Switch> 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 40: 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.

Field	Description
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.
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:

```
Switch> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan summary** command:

```
Switch> 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:

```
Switch# 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
```

Related Topics

[switchport mode
vlan](#), on page 1121

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 switch.
devices		Displays information about all VTP version 3 devices in the domain. This keyword applies only if the switch 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 switch is in VTP transparent or VTP off mode.
interface		Displays VTP status and configuration for all interfaces or the specified interface.
<i>interface-id</i>		(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 switch 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 switch, the password appears in clear text.
- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the switch, 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 switches in the same domain do not have the same primary server for a database.

```
Switch# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf switch ID      Primary Server Revision  System Name
-----
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.

```
Switch> 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
-----
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 41: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this switch 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 switch 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 switch on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.

Field	Description
Summary advertisements transmitted	Number of summary advertisements sent by this switch 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 switch on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this switch 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	<p>Number of revision errors.</p> <p>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 switch increments.</p> <p>Revision errors increment whenever the switch receives an advertisement whose revision number matches the revision number of the switch, but the MD5 digest values do not match. This error means that the VTP password in the two switches is different or that the switches have different configurations.</p> <p>These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>
Number of configuration digest errors	<p>Number of MD5 digest errors.</p> <p>Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the switch do not match. This error usually means that the VTP password in the two switches is different. To solve this problem, make sure the VTP password on all switches is the same.</p> <p>These errors indicate that the switch is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</p>

Field	Description
Number of V1 summary errors	Number of Version 1 errors. Version 1 summary errors increment whenever a switch in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring switch is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the switches in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
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.

```
Switch> 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 42: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the switch.
VTP Version running	Displays the VTP version operating on the switch. By default, the switch implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the switch.

Field	Description
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.
Configuration last modified	Displays the date and time of the last configuration modification. Displays the IP address of the switch that caused the configuration change to the database.
VTP Operating Mode	<p>Displays the VTP operating mode, which can be server, client, or transparent.</p> <p>Server—A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The switch guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every switch is a VTP server.</p> <p>Note The switch 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.</p> <p>Client—A switch 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.</p> <p>Transparent—A switch 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 switch receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</p>
Maximum VLANs Supported Locally	Maximum number of VLANs supported locally.
Number of Existing VLANs	Number of existing VLANs.

Field	Description
Configuration Revision	Current configuration revision number on this switch.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a switch running VTP version 3:

```
Switch> 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 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 0x00

Feature UNKNOWN:
-----
```

Related Topics

[clear vtp counters](#), on page 1095

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	<i>group-name</i> 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:

```
Switch# 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	trust
	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.	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 switch 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 switch 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 switch interfaces.)

You should configure voice VLAN on switch 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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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 <i>vlan-list</i>	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 <i>vlan-list</i> choices.
native vlan <i>vlan-id</i>	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 <i>vlan-list</i>	Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the <i>vlan-list</i> 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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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:

```
Switch(config)# interface gigabitethernet1/0/2
Switch(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.

Related Topics

[show interfaces](#), on page 121

[switchport mode](#)

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	<i>vlan-id</i>	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.
	<i>group word</i> 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 switch 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 switch, 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**—Source-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 switch supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other switches. 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 43: Valid Commands and Syntax for Different Media Types

Media Type	Valid Syntax
Ethernet	name <i>vlan-name</i> , media ethernet, state {suspend active}, said <i>said-value</i> , remote-span , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI	name <i>vlan-name</i> , media fddi, state {suspend active}, said <i>said-value</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
FDDI-NET	name <i>vlan-name</i> , media fd-net, state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieec ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i> If VTP v2 mode is disabled, do not set the stp type to auto .
Token Ring	VTP v1 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring concentrator relay function (TrCRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tokenring, state {suspend active}, said <i>said-value</i> , ring <i>ring-number</i> , parent <i>parent-vlan-id</i> , bridge type {srb srt}, are <i>are-number</i> , ste <i>ste-number</i> , backupcrf {enable disable}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring-NET	VTP v1 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieec ibm}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>
Token Ring bridge relay function (TrBRF)	VTP v2 mode is enabled. name <i>vlan-name</i> , media tr-net, state {suspend active}, said <i>said-value</i> , bridge <i>bridge-number</i> , stp type {ieec ibm auto}, tb-vlan1 <i>tb-vlan1-id</i> , tb-vlan2 <i>tb-vlan2-id</i>

The following table describes the rules for configuring VLANs:

Table 44: 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.
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:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
Switch(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 switch startup configuration file:

```
Switch(config)# vlan 2000  
Switch(config-vlan)# end  
Switch# copy running-config startup config
```

This example shows how to create a VLAN group.

```
Switch(config)# vlan group xyz vlan-list 50-60
```

This example shows how to remove a VLAN group.

```
Switch(config)# no vlan group xyz vlan-list 50-60
```

This example shows how to remove a single VLAN from the VLAN group.

```
Switch(config)# no vlan group xyz vlan-list 51
```

This example shows how to remove multiple VLANs from the VLAN group.

```
Switch(config)# no vlan group xyz vlan-list 52-55
```

This example shows how to remove both single and multiple VLANs from the VLAN group.

```
Switch(config)# no vlan group xyz vlan-list 56, 58-60
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

Related Topics

[show vlan](#), on page 1107

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 switches 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:

```
Switch# configure terminal
Switch (config)# vlan dot1q tag native
Switch (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

Related Topics

[show vlan](#), on page 1107

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 <i>domain-name</i>	Specifies the VTP domain name, an ASCII string from 1 to 32 characters that identifies the VTP administrative domain for the switch. The domain name is case sensitive.
file <i>filename</i>	Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.
interface <i>interface-name</i>	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 switch in VTP client mode. A switch 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 switch 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 switch in VTP off mode. A switch 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 switch in VTP server mode. A switch in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the switch. The switch can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.
transparent	Places the switch in VTP transparent mode. A switch 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 switch 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 switch running configuration file, and you can save them in the switch 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 <i>password</i>	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 switch.
version <i>number</i>	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 switch startup configuration file and reboot the switch, 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 switch is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the switch does not send any VTP advertisements even if changes occur to the local VLAN configuration. The switch 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 switch receives its domain from a summary packet, it resets its configuration revision number to 0. After the switch 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 switch 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 switch is not in client or transparent mode.
- If the receiving switch is in client mode, the client switch changes its configuration to duplicate the configuration of the server. If you have switches in client mode, be sure to make all VTP or VLAN configuration changes on a switch in server mode, as it has a higher VTP configuration revision number. If the receiving switch is in transparent mode, the switch configuration is not changed.
- A switch in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a switch in transparent mode, the changes are not propagated to other switches in the network.
- If you change the VTP or VLAN configuration on a switch that is in server mode, that change is propagated to all the switches in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the switch.
- 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 switches in the same domain.
- When you use the **no vtp password** form of the command, the switch 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 switch automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP switches in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all switches in a domain are VTP Version 2-capable, you only need to configure Version 2 on one switch; the version number is then propagated to the other Version-2 capable switches 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 switch configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Switch(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Switch(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:

```
Switch(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the switch:

```
Switch(config)# vtp domain OurDomainName
```

This example shows how to place the switch in VTP transparent mode:

```
Switch(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Switch(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Switch(config)# vtp pruning
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Switch(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Topics

[show vtp](#), on page 1110

[vtp \(interface configuration\)](#), on page 1133

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 switch is running VTP Version 3.

This example shows how to enable VTP on an interface:

```
Switch(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Switch(config-if)# no vtp
```

Related Topics

[switchport trunk](#), on page 1118

[vtp \(global configuration\)](#), on page 1128

vtp primary

To configure a switch 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 switch as the primary VTP server for the multiple spanning tree (MST) feature.
vlan	(Optional)	Configures the switch as the primary VTP server for VLANs.
force	(Optional)	Configures the switch to not check for conflicting devices when configuring the primary server.

Command Default The switch 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 switch is running VTP Version 3.

This example shows how to configure the switch as the primary VTP server for VLANs:

```
Switch# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

Related Topics

[show vtp](#), on page 1110

[vtp \(global configuration\)](#), on page 1128

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	<i>vlan-id</i> (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	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>Cisco IOS XE 3.2SE</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				
Usage Guidelines	<p>Use this command in the global configuration mode only.</p> <p>This example shows how to enable broadcasting on VLAN 20:</p> <pre>Switch(config)# wireless broadcast vlan 20</pre>				



PART **XV**

WLAN

- [WLAN Commands, on page 1139](#)



WLAN Commands

- [aaa-override](#), on page 1141
- [accounting-list](#), on page 1142
- [assisted-roaming](#), on page 1143
- [ap name ap-name lan port-id port-id poe](#), on page 1144
- [ap name ap-name lan override](#), on page 1145
- [band-select](#), on page 1146
- [broadcast-ssid](#), on page 1147
- [call-snoop](#), on page 1148
- [channel-scan defer-priority](#), on page 1149
- [channel-scan defer-time](#), on page 1150
- [chd](#), on page 1151
- [client association limit](#), on page 1152
- [client vlan](#), on page 1154
- [ccx aironet-iesupport](#), on page 1155
- [datalink flow monitor](#), on page 1156
- [device-classification](#), on page 1157
- [default](#), on page 1158
- [dtim dot11](#), on page 1161
- [exclusionlist](#), on page 1162
- [exit](#), on page 1163
- [exit \(WLAN AP Group\)](#), on page 1164
- [ip access-group](#), on page 1165
- [ip flow monitor](#), on page 1166
- [ip verify source mac-check](#), on page 1167
- [load-balance](#), on page 1168
- [mobility anchor](#), on page 1169
- [nac](#), on page 1171
- [passive-client](#), on page 1172
- [peer-blocking](#), on page 1173
- [port](#), on page 1174
- [poe](#), on page 1175
- [radio](#), on page 1176
- [radio-policy](#), on page 1177

- [remote-lan](#), on page 1178
- [remote-lan](#), on page 1179
- [roamed-voice-client re-anchor](#), on page 1180
- [security ft](#), on page 1181
- [security pmf](#), on page 1183
- [security web-auth](#), on page 1185
- [security wpa akm](#), on page 1186
- [service-policy \(WLAN\)](#), on page 1188
- [session-timeout](#), on page 1189
- [show remote-lan all](#), on page 1190
- [show remote-lan id](#), on page 1191
- [show remote-lan name](#), on page 1192
- [show remote-lan summary](#), on page 1193
- [show running-config remote-lan](#), on page 1194
- [show wlan](#), on page 1195
- [show wireless wlan summary](#), on page 1198
- [shutdown](#), on page 1199
- [sip-cac](#), on page 1200
- [static-ip tunneling](#), on page 1201
- [vlan](#), on page 1202
- [universal-admin](#), on page 1203
- [wgb non-cisco](#), on page 1204
- [wifidirect policy](#), on page 1205
- [wlan \(AP Group Configuration\)](#), on page 1206
- [wlan](#), on page 1207
- [wlan shutdown](#), on page 1208
- [wmm](#), on page 1209

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable AAA on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no aaa-override
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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	<i>radius-server-acct</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# accounting-list test
Switch(config-wlan)# end
```

This example shows how to disable RADIUS server accounting on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no accounting-list test
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch(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:

```
Switch(config)#wlan test-prediction 2 test-prediction
Switch(config-wlan)#client vlan 43
Switch(config-wlan)#no security wpa
Switch(config-wlan)#load-balance
Switch(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.
```

ap name ap-name lan port-id port-id poe

To enable PoE in the LAN port of AP, use the **ap name ap-name lan port-id port-id poe** command in privileged EXEC mode. To disable PoE in the LAN port of AP, use **no** form of this command.



Note PoE can be configured only for port 1.

ap name *ap-name* **lan port-id** *port-id* **poe**

ap name *ap-name* **no lan port-id** *port-id* **poe**

Syntax Description

ap-name Name of the AP.

port-id ID of the port.

Command Default

By default, PoE is disabled.

Command Modes

privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to enable PoE in the LAN port of AP:

```
Switch # ap name AP00FE.C82D.DFB0 lan port-id 1 poe
```

ap name ap-name lan override

To override AP group LAN port configurations, use the **ap name ap-name lan override** command in privileged EXEC mode. To disable Override in an AP group LAN port configuration, use **no** form of this command.

ap name *ap-name* **lan override**

ap name *ap-name* **no lan override**

Syntax Description

ap-name Name of the AP.

Command Default

By default, LAN override is disabled.



Note

The LAN port configurations for each of the AP is allowed only when the LAN override is enabled.

Command Modes

privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to enable Override in an AP group LAN port configuration:

```
Switch # ap name AP00FE.C82D.DFBO lan override
```

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# band-select
Switch(config-wlan)# end
```

This example shows how to disable band selection on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no band-select
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# broadcast-ssid
Switch(config-wlan)# end
```

This example shows how to disable a broadcast SSID on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no broadcast-ssid
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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 WLAN 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# call-snoop
Switch(config-wlan)# end
```

This example shows how to disable VoIP on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no call-snoop
Switch(config-wlan)# end
```

Related Topics

[service-policy \(WLAN\)](#), on page 596
[wlan](#), on page 1207

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	<i>priority</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-priority 4
Switch(config-wlan)# end
```

This example shows how to disable channel scan defer priority on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-priority 4
Switch(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	<i>msecs</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# channel-scan defer-time 300
Switch(config-wlan)# end
```

This example shows how to disable channel scan defer time on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no channel-scan defer-time
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# chd
Switch(config-wlan)# end
```

This example shows how to disable coverage hole detection on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no chd
Switch(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		
	<i>association-limit</i>	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.
	<i>ap-limit</i>	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.
	<i>max-ap-radio-limit</i>	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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# client association limit 200
```

```
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable a client association limit on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no client association limit
Switch(config-wlan)# no shutdown
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit radio 200
Switch(config-wlan)# no shutdown
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client association limit ap 300
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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	<i>interface-id-name-or-group-name</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# client vlan client-vlan1
Switch(config-wlan)# end
```

This example shows how to disable a client VLAN on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no client vlan
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ccx aironet-iesupport
Switch(config-wlan)# end
```

This example shows how to disable an Aironet IE on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no ccx aironet-iesupport
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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	
	<i>datalink-monitor-name</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# datalink flow monitor test output
Switch(config-wlan)# end
```

This example shows how to disable NetFlow monitoring on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no datalink flow monitor test output
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# device-classification
Switch(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|chd|client|datalink|diag-channel|dtim|exclusionlist|ip|ipv6|load-balance|local-auth|mac-filtering|media-stream|mfp}
```

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:

```
Switch(config-wlan)# default ccx aironet-iesupport
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# dtim dot11 24ghz 3
```

This example shows how to disable the DTIM period on a WLAN on the 2.4-GHz band:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no dtim dot11 24ghz 3
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exclusionlist timeout 345
```

This example shows how to disable a client exclusion list on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# exit
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ap group test
Switch(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.				
	<i>acl-name</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to configure a WLAN ACL:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(config-wlan)#ip access-group test-acl
```

This example shows how to configure an IPv4 WLAN web ACL:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip access-group web test
Switch(config-wlan)#
```

Related Topics

[wlan](#), on page 1207

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	
	<i>ip-monitor-name</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip flow monitor test input
```

This example shows how to disable an IP flow monitor:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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 switch, this traffic is dropped in the hardware. IPSG is not supported on DHCP packets. IPSG is not supported for foreign clients in a foreign switch.

You must disable the WLAN before using this command.

This example shows how to enable IPSG:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# ip verify source mac-check
```

This example shows how to disable IPSG:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

This example shows how to disable load balancing on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# shutdown
Switch(config)# wlan wlan1
Switch(config-wlan)# no load-balance
Switch(config)# no shutdown
Switch(config-wlan)# end
```

Related Topics

[wlan](#), on page 1207

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 switch 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:

```
Switch(config-wlan)# mobility anchor sticky
```

This example shows how to configure guest anchoring:

```
Switch(config-wlan)# mobility anchor 209.165.200.224
```

This example shows how to configure the device as an auto-anchor:

```
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# aaa-override
Switch(config-wlan)# nac
```

This example shows how to disable RADIUS NAC on the WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no nac
Switch(config-wlan)# no aaa-override
```

Related Topics

[aaa-override](#), on page 1141

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# passive-client
```

This example shows how to disable the passive client feature on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wireless multicast
Switch(config)# wlan test-wlan
Switch(config-wlan)# no passive-client
```

Related Topics

[wlan](#), on page 1207

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 switch to discard the packets.
	forward-upstream	Specifies the packets to be forwarded on the upstream VLAN. The device next in the hierarchy to the switch 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# peer-blocking drop
Switch(config-wlan)# peer-blocking forward-upstream
```

This example shows how to disable the drop and forward-upstream options for peer-to-peer blocking:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no peer-blocking drop
Switch(config-wlan)# no peer-blocking forward-upstream
```

Related Topics

[wlan](#), on page 1207

port

To configure port id of an AP group, use the **port** command in interface configuration mode.

port *port-id*

Syntax Description	<i>port-id</i> ID of the port.				
Command Default	None				
Command Modes	Interface configuration (config-apgroup)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

The following example shows how to configure port id of an AP group:

```
Switch(config-apgroup)# port 1
```

poe

To enable PoE on a port, use the **poe** command in interface configuration mode.



Note PoE can be configured only for port 1.

poe
no poe

Command Default By default, PoE is disabled.

Command Modes Interface configuration (config-port-apgroup)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to enable PoE on a port:

```
Switch(config-port-apgroup) # poe
```

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# radio all
```

This example shows how to disable all radio bands on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no radio all
```

Related Topics

[wlan](#), on page 1207

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:

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# radio-policy dot11b
```

This example shows how to disable the radio policy on the 802.11b band of an AP group:

```
Switch(config)# ap group test
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# no radio-policy dot11bg
```

Related Topics

[wlan](#), on page 1207

[wlan shutdown](#), on page 1208

remote-lan

To specify Remote-LAN profile name, use the **remote-lan** command in global configuration mode. To disable the configured profile name, use **no** form of this command.

remote-lan *profile-name id*
no remote-lan *profile-name id*

Syntax Description	<i>profile-name</i>	Remote-LAN profile name.
	<i>id</i>	Remote LAN identifier. The range is from 1 to 64.
Command Default	None	
Command Modes	Global configuration (config)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to specify Remote-LAN profile name:

```
Switch(config)# remote-lan test-lan 3
```

remote-lan

To add a Remote-LAN to an AP group, use the **remote-lan** command in interface configuration mode. To remove a Remote-LAN from an AP group, use **no** form of this command.

remote-lan *remote-lan-name*
no remote-lan *remote-lan-name*



Note The **remote-lan remote-lan-name** command is also required to map a Remote-LAN to a port.

Syntax Description	<i>remote-lan-name</i> Name of the Remote-LAN.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Interface configuration (config-apgroup)
----------------------	--

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to add a Remote-LAN to an AP group:

```
Switch(config-apgroup) # remote-lan test-lan
```

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# roamed-voice-client re-anchor
```

This example shows how to disable the roamed voice client re-anchor feature:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no roamed-voice-client re-anchor
```

Related Topics

[wlan](#), on page 1207

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.
	<i>timeout-in-seconds</i>	(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:

```
Switch#wlan test
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no mobility anchor sticky
Switch(config-wlan)# no security wpa
Switch(config-wlan)# no security wpa akm dot1x
Switch(config-wlan)# no security wpa wpa2
Switch(config-wlan)# no security wpa wpa2 ciphers aes
Switch(config-wlan)# security ft
Switch(config-wlan)# shutdown
```

The following example shows a sample security FT on a WPA-enabled WLAN:

```
Switch# wlan test
Switch(config-wlan)# client vlan 0140
Switch(config-wlan)# no security wpa akm dot1x
Switch(config-wlan)# security wpa akm ft psk
Switch(config-wlan)# security wpa akm psk set-key ascii 0 test-test
```

```
Switch(config-wlan)# security ft
Switch(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.
	<i>association-comeback-time-seconds</i>	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 switch does not get a response, another SA query is tried.
	<i>saquery-retry-time-milliseconds</i>	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 (switch) 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.

```
Switch(config-wlan)# security pmf association-comeback 15
```

This example shows how to configure mandatory 802.11w MPF protection for clients on a WLAN:

```
Switch(config-wlan)# security pmf mandatory
```

This example shows how to configure optional 802.11w MPF protection for clients on a WLAN:

```
Switch(config-wlan)# security pmf optional
```

This example shows how to configure the saquery parameter:

```
Switch(config-wlan)# security pmf saquery-retry-time 100
```

This example shows how to disable the PMF feature:

```
Switch(config-wlan)# no security pmf
```

Related Topics

[security wpa akm](#), on page 1186

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 <i>authentication-list-name</i>	Sets the authentication list for IEEE 802.1x.	
on-macfilter-failure	Enables web authentication on MAC failure.	
parameter-map <i>parameter-map-name</i>	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:

```
Switch(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|tkip}}]]
no security wpa [{akm {cckm|dot1x|ft|pmf|psk}}|wpa1 [ciphers {aes|tkip}}|wpa2 [ciphers {aes|tkip}}]]
```

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.

```
Switch(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.

Examples

This example shows how to configure the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy input policy-test
```

This example shows how to disable the input QoS service policy on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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):

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# service-policy output platinum
```

Related Topics

[wlan](#), on page 1207

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	<i>seconds</i> 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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

This example shows how to configure a session timeout to 300 seconds:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# session-timeout 300
```

This example shows how to disable a session timeout:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no session-timeout
```

show remote-lan all

To display Remote-LAN properties of all configured Remote-LANs, use the **show remote-lan all** command.

show remote-lan all

Syntax Description	This command has no keywords or arguments.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example displays Remote-LAN properties of all configured Remote-LANs:

```
Switch#show remote-lan all
Remote-LAN Profile Name : test
=====
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
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
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan id

To display the Remote-LAN configuration by ID, use the **show remote-lan id** command.

show remote-lan id *id*

Syntax Description	<i>id</i> Remote LAN identifier. The range is from 1 to 64.				
Command Default	None				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

The following example shows how to display the Remote-LAN configuration by ID:

```
Switch #show remote-lan id 2
Remote-LAN Profile Name      : test
=====
Identifier                    : 2
Status                        : Disabled
Universal AP Admin           : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override          : Enabled
Number of Active Clients     : 0
Exclusionlist Timeout        : 21474
Session Timeout              : 864 seconds
Interface                    : default
Interface Status             : Up
Remote-LAN ACL               : testacl
DHCP Server                  : 10.5.7.9
DHCP Address Assignment Required : Disabled
Local EAP Authentication     : testeaprofile
Mac Filter Authorization list name : testmaclist
Accounting list name         : testlist
802.1x authentication list name : dotxauth
Security
  802.11 Authentication      : Open System
  802.1X                     : Enabled
  Encryption                 : 104-bit WEP
```

show remote-lan name

To display Remote-LAN configuration by profile name, use the **show remote-lan name** command.

show remote-lan name *name*

Syntax Description	<i>name</i> Remote-LAN profile name.				
Command Default	None				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

The following example shows how to display Remote-LAN configuration by profile name:

```
Switch# show remote-lan name test
Remote-LAN Profile Name : test
=====
Identifier : 1
Status : Disabled
Universal AP Admin : Disabled
Max Associated Clients per Remote-LAN : 0
AAA Policy Override : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
Interface : default
Interface Status : Up
Remote-LAN ACL : unconfigured
DHCP Server : 0.0.0.0
DHCP Address Assignment Required : Disabled
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
802.1X : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
```

show remote-lan summary

To display the summary of all Remote-LANs, use the **show remote-lan summary** command.

show remote-lan summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

The following example shows how to display the summary of all Remote-LANs:

```
Switch # show remote-lan summary
Number of Remote-LANs: 1
```

Remote-LAN	Profile Name	VLAN	Status
2	test	1	DOWN

show running-config remote-lan

To display Remote-LAN configuration, use the **show running-config remote-lan** command.

show running-config remote-lan *name*

Syntax Description	<i>name</i> Remote-LAN profile name.				
Command Default	None				
Command Modes	Privileged EXEC (#)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.3.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.3.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.3.1	This command was introduced.				

The following example shows how to display Remote-LAN configuration:

```
Switch# show running-config remote-lan test
remote-lan test 1
aaa-override
accounting-list test-all-list
exclusionlist timeout 100
ip access-group test-acl
ip dhcp server 10.100.12.5
mac-filtering test-mac-list
security dot1x authentication-list test-dot1x-list
session-timeout 100
shutdown
```

show wlan

To view WLAN parameters, use the **show wlan** command.

```
show wlan {all |id wlan-id|name wlan-name |summary}
```

Syntax Description	all	Description
	all	Displays a summary of parameters of all configured WLANs. The list is ordered by the ascending order of the WLAN IDs.
	id <i>wlan-id</i>	Specifies the wireless LAN identifier. The range is from 1 to 512.
	name <i>wlan-name</i>	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:

```
Switch# 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:

```
Switch# 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)
    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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>15.2(3)E</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	15.2(3)E	This command was introduced.
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 Status	SSID	Security	Radio	VLAN	Client
1	Test1 DOWN	xxx	WPA1/WPA2	All	1	0
2	wlan1 DOWN	wlan2-ssid	WPA1/WPA2	All	1	0
3	wlan3 DOWN	mywlan3	WPA1/WPA2	All	1	0

shutdown

To disable a WLAN, use the **shutdown** command. To enable a WLAN, use the **no** form of this command.

shutdown
no shutdown



Note To enable LAN port in an AP group configuration and Remote-LAN profile, use the **no** form of this command.

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# shutdown
Switch(config-wlan)# end
Switch# 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan test-wlan
Switch(config-wlan)# no shutdown
Switch(config-wlan)# end
Switch# 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:

```

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# sip-cac disassoc-client
Switch(config-wlan)# sip-cac send-486busy

```

This example shows how to disable a client association and 486 busy message on a WLAN:

```

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no sip-cac disassoc-client
Switch(config-wlan)# no sip-cac send-486busy

```

Related Topics

[wlan](#), on page 1207

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# static-ip tunneling
```

This example shows how to disable static-IP tunneling:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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	<i>interface-name</i> VLAN interface name.
---------------------------	--

Command Default	No VLAN 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ap group ap-group-1
Switch(config-apgroup)# wlan test-wlan
Switch(config-wlan-apgroup)# vlan 3
```

Related Topics

[wlan](#), on page 1207

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.

```

Switchenable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#wlan wlan1
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# wgb non-cisco
Switch(config-wlan)# no shutdown
```

This example shows how to disable support for non-Cisco WGB clients on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
Switch(config-wlan)# no wgb non-cisco
Switch(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	<p>When the Wi-Fi Direct policy is configured as "deny", the switch 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 switch and these are based on the Wi-Fi capabilities of the device. These include:</p> <ul style="list-style-type: none"> • Concurrent Operation • Cross connection <p>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.</p>

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:

```
Switch(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	<i>wlan-name</i> 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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ap group test
Switch(config-apgroup)# wlan qos-wlan
```

Related Topics

[wlan](#), on page 1207

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

<i>wlan-name</i>	WLAN profile name. The name is from 1 to 32 alphanumeric characters.
<i>wlan-id</i>	Wireless LAN identifier. The range is from 1 to 512.
<i>wlan-ssid</i>	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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config)# wlan test-wlan-cr 67 test-wlan-cr-ssid
```

This example shows how to delete a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# shutdown
```

Related Topics

[wlan](#), on page 1207

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	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE 3.2SE</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE 3.2SE	This command was introduced.
Release	Modification				
Cisco IOS XE 3.2SE	This command was introduced.				

Usage Guidelines When the switch 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 switch.

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:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# wmm allowed
```

This example shows how to disable WMM on a WLAN:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# wlan wlan1
Switch(config-wlan)# no wmm
```

Related Topics

[wlan](#), on page 1207

