



Command Reference, Cisco IOS XE Everest 16.5.1a (Catalyst 3850 Switches)

First Published: 2017-05-31

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	xxv
Document Conventions	xxv
Related Documentation	xxvii
Obtaining Documentation and Submitting a Service Request	xxvii

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

Campus Fabric	13
----------------------	-----------

CHAPTER 2**Campus Fabric 15**

- border 16
- context 17
- control-plane 18
- domain 19
- debug fabric auto 20
- fabric auto 21
- host-pool name 22
- show fabric domain 24
- show fabric context 25
- show fabric host-pool 26

PART II**Interface and Hardware Components 27**

CHAPTER 3**Interface and Hardware Commands 29**

- debug ilpower 31
- debug interface 32
- debug lldp packets 33
- debug platform poe 34
- duplex 35
- errdisable detect cause 37
- errdisable recovery cause 39
- errdisable recovery interval 42
- interface 43
- interface range 45
- ip mtu 47
- ipv6 mtu 48
- lldp (interface configuration) 49
- logging event power-inline-status 51
- mdix auto 52
- mode (power-stack configuration) 53
- network-policy 55
- network-policy profile (global configuration) 56

power efficient-ethernet auto	57
power-priority	58
power inline	60
power inline police	64
power supply	66
show eee	68
show env	71
show errdisable detect	74
show errdisable recovery	75
show interfaces	76
show interfaces counters	80
show interfaces switchport	82
show interfaces transceiver	84
show memory platform	87
show module	90
show mgmt-infra trace messages ilpower	91
show mgmt-infra trace messages ilpower-ha	93
show mgmt-infra trace messages platform-mgr-poe	94
show network-policy profile	95
show platform hardware fed switch forward	96
show platform resources	98
show platform software ilpower	99
show platform software process list	101
show platform software process slot switch	103
show platform software status control-processor	105
show processes cpu platform monitor	108
show processes memory platform	110
show power inline	113
show stack-power	119
show system mtu	121
show tech-support	122
speed	124
stack-power	126
switchport block	128

system mtu 129
 test mcu read-register 130
 voice-signaling vlan (network-policy configuration) 132
 voice vlan (network-policy configuration) 134

PART III **IP** 137

CHAPTER 4 **IP** 139

clear ip nhrp 141
 debug nhrp 142
 fhrp delay 144
 fhrp version vrrp v3 145
 glbp authentication 146
 glbp forwarder preempt 148
 glbp ip 149
 glbp load-balancing 151
 glbp name 152
 glbp preempt 154
 glbp priority 155
 glbp timers 156
 glbp weighting 158
 glbp weighting track 159
 ip address dhcp 161
 ip address pool (DHCP) 164
 ip address 165
 ip http server 168
 ip http secure-server 170
 ip nhrp map 172
 ip nhrp map multicast 174
 ip nhrp network-id 176
 ip nhrp nhs 177
 ipv6 nd cache expire 179
 ipv6 nd na glean 180
 ipv6 nd nud retry 181

- key chain 183
- key-string (authentication) 184
- key 185
- show glbp 187
- show ip nhrp nhs 190
- show ip ports all 192
- show key chain 194
- show track 195
- track 197
- vrrp 199
- vrrp description 200
- vrrp preempt 201
- vrrp priority 202
- vrrp timers advertise 203
- vrrs leader 205

PART IV
IP Multicast Routing 207

CHAPTER 5
IP Multicast Routing 209

- cache-memory-max 211
- clear ip mfib counters 212
- clear ip mroute 213
- ip igmp filter 214
- ip igmp max-groups 215
- ip igmp profile 217
- ip igmp snooping 218
- ip igmp snooping last-member-query-count 219
- ip igmp snooping querier 221
- ip igmp snooping report-suppression 223
- ip igmp snooping vlan mrouter 224
- ip igmp snooping vlan static 225
- ip multicast auto-enable 226
- ip pim accept-register 227
- ip pim bsr-candidate 228

ip pim rp-candidate	230
ip pim send-rp-announce	231
ip pim spt-threshold	233
match message-type	234
match service-type	235
match service-instance	236
mrinfo	237
redistribute mdns-sd	239
service-list mdns-sd	240
service-policy-query	241
service-routing mdns-sd	242
service-policy	243
show ip igmp filter	244
show ip igmp profile	245
show ip igmp snooping	246
show ip igmp snooping groups	248
show ip igmp snooping mrouter	250
show ip igmp snooping querier	251
show ip pim autorp	253
show ip pim bsr-router	254
show ip pim bsr	255
show ip pim tunnel	256
show mdns cache	258
show mdns requests	260
show mdns statistics	261
show platform software fed switch ip multicast	262

PART V **IPv6** **265**

CHAPTER 6 **IPv6** **267**

ipv6 dhcp server vrf enable	268
ipv6 flow monitor	269
show ipv6 dhcp binding	270

PART VI**Layer 2/3 273**

CHAPTER 7**Layer 2/3 275**

- channel-group 277
- channel-protocol 280
- clear lacp 281
- clear pagp 282
- clear spanning-tree counters 283
- clear spanning-tree detected-protocols 284
- debug etherchannel 285
- debug lacp 286
- debug pagp 287
- debug platform pm 288
- debug platform ulld 290
- debug spanning-tree 291
- interface port-channel 293
- lacp max-bundle 294
- lacp port-priority 295
- lacp rate 296
- lacp system-priority 297
- pagp learn-method 298
- pagp port-priority 300
- port-channel 301
- port-channel auto 302
- port-channel load-balance 303
- port-channel load-balance extended 305
- port-channel min-links 306
- rep admin vlan 307
- rep block port 308
- rep lsl-age-timer 310
- rep lsl-retries 311
- rep preempt delay 312
- rep preempt segment 313

rep segment	314
rep stcn	316
show etherchannel	317
show interfaces rep detail	320
show lacp	321
show pagp	325
show platform software fed etherchannel	327
show platform pm	328
show rep topology	329
show udld	331
switchport	334
switchport access vlan	336
switchport mode	339
switchport nonegotiate	341
switchport voice vlan	342
udld	345
udld port	347
udld reset	349

PART VII**Multiprotocol Label Switching (MPLS)** 351

CHAPTER 8**MPLS** 353

mpls ip default-route	354
mpls ip (global configuration)	355
mpls ip (interface configuration)	356
mpls label protocol (global configuration)	357
mpls label protocol (interface configuration)	358
mpls label range	359
show mpls label range	361

CHAPTER 9**Multicast VPN** 363

ip multicast-routing	364
ip multicast mrimo-filter	365
mdt data	366

- mdt default 368
- mdt log-reuse 370
- show ip pim mdt bgp 371
- show ip pim mdt history 372
- show ip pim mdt receive 373
- show ip pim mdt send 375

PART VIII**Network Management 377**

CHAPTER 10**Flexible NetFlow 379**

- cache 381
- clear flow exporter 384
- clear flow monitor 385
- collect 387
- collect counter 388
- collect interface 389
- collect timestamp absolute 390
- collect transport tcp flags 391
- datalink flow monitor 392
- debug flow exporter 393
- debug flow monitor 394
- debug flow record 395
- debug sampler 396
- description 397
- destination 398
- dscp 399
- export-protocol netflow-v9 400
- exporter 401
- flow exporter 402
- flow monitor 403
- flow record 404
- ip flow monitor 405
- ipv6 flow monitor 407
- match datalink dot1q priority 409

match datalink dot1q vlan	410
match datalink ethertype	411
match datalink mac	412
match datalink vlan	413
match flow cts	414
match flow direction	415
match interface	416
match ipv4	417
match ipv4 destination address	418
match ipv4 source address	419
match ipv4 ttl	420
match ipv6	421
match ipv6 destination address	422
match ipv6 hop-limit	423
match ipv6 source address	424
match transport	425
match transport icmp ipv4	426
match transport icmp ipv6	427
mode random 1 out-of	428
option	429
record	431
sampler	432
show flow exporter	433
show flow interface	435
show flow monitor	437
show flow record	442
show sampler	443
source	445
template data timeout	447
transport	448
ttl	449

CHAPTER 11**Network Management 451**

description (ERSPAN)	453
----------------------	-----

destination (ERSPAN)	454
erspan-id	456
filter (ERSPAN)	457
ip ttl (ERSPAN)	459
ip wccp	460
monitor capture (interface/control plane)	462
monitor capture buffer	466
monitor capture clear	467
monitor capture export	468
monitor capture file	469
monitor capture limit	471
monitor capture match	472
monitor capture start	473
monitor capture stop	474
monitor session	475
monitor session destination	477
monitor session filter	481
monitor session source	483
monitor session type erspan-source	485
origin	486
show ip sla statistics	488
show capability feature monitor	490
show monitor	491
show monitor capture	493
show monitor session	495
show platform software fed switch ip wccp	497
show platform ip wccp	499
show platform software swspan	500
snmp-server enable traps	502
snmp-server enable traps bridge	505
snmp-server enable traps bulkstat	506
snmp-server enable traps call-home	507
snmp-server enable traps cef	508
snmp-server enable traps cpu	509

snmp-server enable traps envmon 510

snmp-server enable traps errdisable 511

snmp-server enable traps flash 512

snmp-server enable traps isis 513

snmp-server enable traps license 514

snmp-server enable traps mac-notification 515

snmp-server enable traps ospf 516

snmp-server enable traps pim 517

snmp-server enable traps port-security 518

snmp-server enable traps power-ethernet 519

snmp-server enable traps snmp 520

snmp-server enable traps stackwise 521

snmp-server enable traps storm-control 523

snmp-server enable traps stpx 524

snmp-server enable traps transceiver 525

snmp-server enable traps vrfmib 526

snmp-server enable traps vstack 527

snmp-server engineID 528

snmp-server host 529

source (ERSPAN) 533

switchport mode access 534

switchport voice vlan 535

PART IX Programmability 537

CHAPTER 12 Programmability 539

boot ipxe 540

boot manual 541

boot system 542

default boot 543

install 544

show install 548

dig 550

mlog 552

[net-debug](#) 553
[net-dhcp](#) 555
[net6-dhcp](#) 556
[net-show](#) 557
[net6-show](#) 558
[net-tcp-bufs](#) 559
[net-tcp-mss](#) 560
[ping](#) 561
[ping4](#) 562
[ping6](#) 563

PART X
QoS 565

CHAPTER 13
Auto-QoS 567

[auto qos classify](#) 568
[auto qos trust](#) 574
[auto qos video](#) 582
[auto qos voip](#) 593
[debug auto qos](#) 606
[show auto qos](#) 607

CHAPTER 14
QoS 609

[class](#) 610
[class-map](#) 613
[match \(class-map configuration\)](#) 615
[match non-client-nrt](#) 618
[policy-map](#) 619
[priority](#) 621
[queue-buffers ratio](#) 623
[queue-limit](#) 624
[service-policy \(Wired\)](#) 626
[set](#) 628
[show class-map](#) 634
[show platform hardware fed switch](#) 635

show platform software fed switch qos 638
 show platform software fed switch qos qsb 639
 show policy-map 642
 trust device 644

PART XI

Routing 647

CHAPTER 15

Bidirectional Forwarding Detection 649

authentication (BFD) 650
 bfd 651
 bfd all-interfaces 653
 bfd check-ctrl-plane-failure 654
 bfd echo 655
 bfd slow-timers 657
 bfd template 659
 bfd-template 660
 ip route static bfd 661
 ipv6 route static bfd 663

PART XII

Security 665

CHAPTER 16

Security 667

aaa accounting 670
 aaa accounting dot1x 673
 aaa accounting identity 675
 aaa authentication dot1x 677
 aaa authorization 678
 aaa authorization network 682
 aaa new-model 683
 aaa policy interface-config allow-subinterface 685
 access-session mac-move deny 686
 access-session template monitor 688
 action 689
 authentication host-mode 690

authentication mac-move permit	692
authentication priority	694
authentication violation	697
cisp enable	699
clear errdisable interface vlan	700
clear mac address-table	701
cts manual	703
cts role-based enforcement	704
cts role-based l2-vrf	706
cts role-based monitor	708
cts role-based permissions	709
deny (MAC access-list configuration)	710
device-role (IPv6 snooping)	714
device-role (IPv6 nd inspection)	715
device-tracking policy	716
dot1x critical (global configuration)	718
dot1x max-start	719
dot1x pae	720
dot1x supplicant controlled transient	721
dot1x supplicant force-multicast	722
dot1x test eapol-capable	723
dot1x test timeout	724
dot1x timeout	725
epm access-control open	727
ip access-list role-based	728
ip admission	729
ip admission name	730
ip device tracking maximum	732
ip device tracking probe	733
ip dhcp snooping database	734
ip dhcp snooping information option format remote-id	736
ip dhcp snooping verify no-relay-agent-address	737
ip http access-class	738
ip radius source-interface	740

ip source binding	742
ip verify source	743
ipv6 access-list	744
ipv6 snooping policy	746
key chain macsec	747
limit address-count	748
mab request format attribute 32	749
macsec network-link	751
match (access-map configuration)	752
mka policy (global configuration)	754
mka pre-shared-key	756
no authentication logging verbose	757
no dot1x logging verbose	758
no mab logging verbose	759
permit (MAC access-list configuration)	760
propagate sgt (cts manual)	764
protocol (IPv6 snooping)	766
radius server	767
sap mode-list (cts manual)	769
security level (IPv6 snooping)	771
security passthru	772
server-private (RADIUS)	773
show aaa clients	775
show aaa command handler	776
show aaa local	777
show aaa servers	778
show aaa sessions	779
show authentication history	780
show authentication sessions	781
show cts interface	784
show cts role-based permissions	786
show cisp	788
show dot1x	790
show eap pac peer	792

show ip dhcp snooping statistics	793
show macsec	796
show mka policy	798
show mka session	801
show mka statistics	804
show mka summary	807
show radius server-group	810
show storm-control	812
show vlan access-map	814
show vlan filter	815
show vlan group	816
storm-control	817
switchport port-security aging	820
switchport port-security mac-address	822
switchport port-security maximum	824
switchport port-security violation	826
tacacs server	828
tracking (IPv6 snooping)	829
trusted-port	831
vlan access-map	832
vlan filter	834
vlan group	835

PART XIII**Stack Manager and High Availability 837**

CHAPTER 17**Stack Manager and High Availability 839**

debug platform stack-manager	840
main-cpu	841
mode sso	842
policy config-sync prc reload	843
redundancy	844
redundancy config-sync mismatched-commands	845
redundancy force-switchover	847
redundancy reload	848

- reload 849
- session 851
- show platform stack-manager 852
- show redundancy 853
- show redundancy config-sync 857
- show switch 859
- stack-mac persistent timer 863
- stack-mac update force 864
- standby console enable 865
- switch stack port 866
- switch priority 867
- switch provision 868
- switch renumber 870

PART XIV**System Management 871**

CHAPTER 18**Autonomic Networking 873**

- autonomic adjacency-discovery 874
- autonomic connect 875
- clear autonomic 876
- debug autonomic 878
- show autonomic control-plane 879
- show autonomic device 881
- show autonomic interfaces 882
- show autonomic intent 884
- show autonomic l2-channels 885
- show autonomic service 886
- show autonomic neighbor 887

CHAPTER 19**System Management Commands 889**

- arp 891
- boot 892
- cat 893
- clear location 894

clear location statistics 895

copy 896

copy startup-config tftp: 897

copy tftp: startup-config 898

debug voice diagnostics mac-address 899

delete 900

dir 901

emergency-install 903

exit 905

flash_init 906

help 907

l2 traceroute 908

license right-to-use 909

location 911

location plm calibrating 914

mac address-table move update 915

mgmt_init 916

mkdir 917

more 918

no debug all 919

rename 920

request platform software console attach switch 921

request platform software package clean 923

request platform software package copy 925

request platform software package describe file 926

request platform software package expand 932

request platform software package install auto-upgrade 934

request platform software package install commit 935

request platform software package install file 936

request platform software package install rollback 939

request platform software package install snapshot 941

request platform software package verify 943

request platform software package uninstall 944

reset 945

rmdir	946
sdm prefer	947
set	948
show avc client	951
show cable-diagnostics tdr	952
show debug	954
show env	955
show env xps	957
show flow monitor	961
show license right-to-use	966
show location	968
show mac address-table move update	969
show platform integrity	970
show platform sudi certificate	971
show sdm prefer	973
system env temperature threshold yellow	975
test cable-diagnostics tdr	977
traceroute mac	978
traceroute mac ip	981
type	983
unset	984
version	986

CHAPTER 20
Tracing 987

Information About Tracing	988
Tracing Overview	988
Location of Tracelogs	988
Tracelog Naming Convention	988
Rotation and Throttling Policy	989
Tracing Levels	989
set platform software trace	990
show platform software trace filter-binary	994
show platform software trace message	995
show platform software trace level	998

request platform software trace archive 1001
 request platform software trace rotate all 1002
 request platform software trace filter-binary 1003

PART XV
VLAN 1005

CHAPTER 21
VLAN 1007

clear l2protocol-tunnel counters 1008
 clear vmps statistics 1009
 clear vtp counters 1010
 debug platform vlan 1011
 debug sw-vlan 1012
 debug sw-vlan ifs 1014
 debug sw-vlan notification 1015
 debug sw-vlan vtp 1016
 interface vlan 1018
 l2protocol-tunnel 1019
 l2protocol-tunnel cos 1022
 private-vlan 1023
 private-vlan mapping 1025
 show dot1q-tunnel 1027
 show interfaces private-vlan mapping 1028
 show l2protocol-tunnel 1029
 show platform vlan 1031
 show vlan 1032
 show vmps 1036
 show vtp 1038
 switchport mode private-vlan 1044
 switchport priority extend 1046
 switchport trunk 1047
 vlan 1050
 vlan dot1q tag native 1056
 vmps reconfirm (global configuration) 1057
 vmps reconfirm (privileged EXEC) 1058

vmps retry 1059
vmps server 1060
vtp (global configuration) 1061
vtp (interface configuration) 1066
vtp primary 1067

Notices 5



Preface

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

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> .
<code>Courier font</code>	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 device, refer to the device 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.	Device#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Device(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switch.

Mode	Access Method	Prompt	Exit Method	About This Mode
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Device (config-vlan) #	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Device (config-if) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the Ethernet ports.
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Device (config-line) #	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

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

Understanding the Help System

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

Table 2: Help Summary

Command	Purpose
help	Obtains a brief description of the help system in any command mode.
<i>abbreviated-command-entry ?</i> Device# 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>Device# sh conf<tab> Device# 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>Device(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:

```
Device# show conf
```

Understanding no and default Forms of Commands

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

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

Understanding CLI Error Messages

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

Table 3: Common CLI Error Messages

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

Using Configuration Logging

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



Note Only CLI or HTTP changes are logged.

Using Command History

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

Changing the Command History Buffer Size

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

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

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

The range is from 0 to 256.

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

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

The range is from 0 to 256.

Recalling Commands

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



Note

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

Table 4: Recalling Commands

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

Disabling the Command History Feature

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

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

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

Using Editing Features

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

Enabling and Disabling Editing Features

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

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

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

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

```
Device# terminal editing
```

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

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

Editing Commands through Keystrokes

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



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

Table 5: Editing Commands through Keystrokes

Capability	Keystroke	Purpose
Move around the command line to make changes or corrections.	Press Ctrl-B , or press the left arrow key.	Moves the cursor back one character.
	Press Ctrl-F , or press the right arrow key.	Moves the cursor forward one character.
	Press Ctrl-A .	Moves the cursor to the beginning of the command line.
	Press Ctrl-E .	Moves the cursor to the end of the command line.
	Press Esc B .	Moves the cursor back one word.
	Press Esc F .	Moves the cursor forward one word.
	Press Ctrl-T .	Transposes the character to the left of the cursor with the character located at the cursor.

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.

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

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

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

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

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

Searching and Filtering Output of show and more Commands

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

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

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

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

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

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

Accessing the CLI

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

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



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

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

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

Accessing the CLI through a Console Connection or through Telnet

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

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

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

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

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

The switch supports up to five simultaneous secure SSH sessions.

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



PART **I**

Campus Fabric

- [Campus Fabric, on page 15](#)



Campus Fabric

- [border](#), on page 16
- [context](#), on page 17
- [control-plane](#), on page 18
- [domain](#), on page 19
- [debug fabric auto](#), on page 20
- [fabric auto](#), on page 21
- [host-pool name](#), on page 22
- [show fabric domain](#), on page 24
- [show fabric context](#), on page 25
- [show fabric host-pool](#), on page 26

border

border *ip address*

Syntax Description	<i>ip address</i> Configures the IP address of the fabric border device.
---------------------------	--

Command Default	None.
------------------------	-------

Command Modes	Fabric-auto-domain configuration
----------------------	----------------------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	Use this command to configure the IP address of the fabric border device. Border devices in the fabric domain connect traditional Layer 3 networks or different fabric domains to the local domain, and translate reachability and policy (VRF and SGT) information from one domain to another. Fabric border devices correspond to proxy egress tunnel routers in LISP.
-------------------------	---

This command auto-generates LISP configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the fabric domain configuration including the auto-generated commands.

Example

The following configuration is auto-generated when this command is run on your device:

```
Device(config-fabric-auto-domain)#border 198.51.100.4
```

```
    ipv4 use-petr 198.51.100.4 priority 10 weight 10
```

For information about the **ipv4 proxy etr** command, see [LISP Command Reference](#).

context

```
context name name id id
```

Syntax Description

context name	Creates a new layer 3 context in the fabric domain.
id id	Assigns an ID to the context.

Command Default

None

Command Modes

Fabric-auto-domain configuration mode

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

A virtual context provides virtualization at the device level, using virtual routing and forwarding (VRF), to create multiple instances of Layer 3 routing tables. Contexts or VRFs provide segmentation across IP addresses, allowing for overlapped address space and traffic separation. \

This command enables the auto-generation of LISP (Locator ID Separation Protocol) and VRF (Virtual Routing and Forwarding) configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the virtual context configuration including the auto-generated base line commands.

Example

```
Device(config-fabric-auto-domain)#context name guest
id 10
```

The following configuration is auto-generated when this command is run on your device:

```
ip vrf guest
  description Auto-provisioned vrf for context example-context (source - fabric auto)
router lisp
  eid-table vrf guest instance-id 10
```

control-plane

control-plane { *ip address* | **auth-key** *key* }

Syntax Description		
	<i>ip address</i>	Configures the IP address of the control-plane device.
	auth-key <i>key</i>	Configures the key to authenticate access to the control-plane device.

Command Default None

Command Modes Fabric-auto-domain configuration mode

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the command to configure the control-plane device IP address and the authentication key, to allow fabric edge devices to communicate with the control-plane device.

This command auto-generates LISP configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the fabric domain configuration including the auto-generated commands.

Example

The following configuration is auto-generated when this command is run on your device:

```
Device(config-fabric-auto-domain)#control-plane 2.2.2.2
auth_key examplekey123

router lisp
locator-set default.RLOC
ipv4-interface Loopback0 priority 10 weight 10
exit

disable-ttl-propagate
ipv4 sgt
eid-table default instance-id 0
exit

loc-reach-algorithm lsb-reports ignore
ipv4 itr map-resolver 2.2.2.2
ipv4 itr
ipv4 etr map-server 2.2.2.2 key examplekey123
ipv4 etr
```

For information about the **ipv4 map-server** and **ipv4 map-resolver** commands, see [LISP Command Reference](#).

domain

Configures the fabric domain and enters fabric-auto-domain configuration mode. The **no** version of this command deletes the fabric domain.

```
domain { default | name name }
no domain
```

Syntax Description

default Configures the default fabric domain and enters fabric-auto domain configuration mode.

name *name* Configures a new fabric domain and enters fabric-auto domain configuration mode.

Command Default

None

Command Modes

Fabric-auto configuration mode

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

We recommend that you use the default domain, unless your network requires you to create a new domain. This command allows you to enter fabric-auto domain configuration mode where you can configure edge, control-plane and border devices in the fabric domain.

Example

```
Device(config-fabric-auto)#domain default
```

```
Device(config-fabric-auto)#domain name exampledomain
```

debug fabric auto

```
debug fabric auto {trace | level | {error | verbose}}
```

Syntax Description	trace	Enables the tracing for the commands auto-generated when the fabric-auto command is executed.
	level error	Displays the errors encountered during Fabric Overlay provisioning.
	level verbose	Displays the maximum number of messages encountered during Fabric Overlay provisioning.

Command Default None.

Command Modes Privileged Exec

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use these debug commands to troubleshoot your fabric domain configuration, and trace the commands auto-generated by the **fabric auto** command, and display the errors encountered.

The no **debug fabric auto level verbose** command disables the display of all the messages encountered during fabric provisioning.

fabric auto

To enable automatic fabric provisioning and enter automatic fabric configuration mode, use the **fabric auto** command in global configuration mode.

fabric auto

Syntax Description	fabric auto Enables automatic fabric provisioning and enters fabric-auto configuration mode.
---------------------------	---

Command Default	None
------------------------	------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	The fabric auto command allows you to configure all the elements in your fabric domain automatically. Additionally, this command enables the auto-generation LISP, VLAN, VRF configuration, to orchestrate the fabric overlay. The show-running configuration command shows the fabric domain configuration including the and auto-generated base line commands.
-------------------------	--

Example

```
Device(config)#fabric auto
```

host-pool name

Creates an IP pool to group endpoints in the fabric domain, and enters host-pool configuration mode.

```
host-pool name name { vlan ID | gateway ipv4 -address/subnet mask | context name name |
use-dhcp ipv4 address }
```

Syntax Description		
	vlan <i>ID</i>	Configures a VLAN ID to associate with the host-pool.
	context name <i>name</i>	Associates a context or a VRF with the host-pool.
	gateway <i>ipv4 address/subnet mask</i>	Configures the routing gateway IP address and subnet mask for the host-pool.
	use-dhcp <i>ipv4 address</i>	Configures a DHCP server for the host-pool.

Command Default None

Command Modes Fabric-auto-domain configuration mode

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the host-pool command to group endpoints in the fabric domain into IP pools, and identify them with a VLAN ID and an IP subnet.

This command auto-generates LISP configuration, to orchestrate the fabric overlay. The **show-running configuration** command shows the fabric domain configuration including the auto-generated commands.

Example

This example configures a host-pool in your fabric domain.

```
device(config-fabric-auto-domain)#host-pool name VOICE_DOMAIN
device(config-fabric-auto-domain-host-pool)#vlan 10
device(config-fabric-auto-domain-host-pool)#context name example-context
device(config-fabric-auto-domain-host-pool)#gateway 192.168.1.254/24
device(config-fabric-auto-domain-host-pool)#use-dhcp 172.10.1.1
device(config-fabric-auto-domain-host-pool)#exit
```

This configuration is auto-generated when you configure a host-pool:

```
ip dhcp relay information option vpn
ip dhcp relay information option
ip dhcp snooping vlan 10
ip dhcp snooping
vlan 10
name VOICE_DOMAIN
interface Vlan10
ip vrf forwarding example-context
ip dhcp relay source-interface Loopback0
```

```
ip address 192.168.1.254 255.255.255.0
ip helper-address global 209.65.201.6
no ip redirects
ip local-proxy-arp
ip route-cache same-interface
no lisp mobility liveness test
lisp mobility example-context.EID.VOICE_DOMAIN
!
router lisp
eid-table vrf example-context
dynamic-eid example-context.EID.VOICE_DOMAIN
database-mapping 192.168.1.0/24 locator-set default.RLOC
```

show fabric domain

show fabric domain

Command Default Default domain and default context

Command Modes Privileged Exec

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the command to display a summary of the fabric domain. The following is sample output for an edge device.

```
device#show fabric domain
Fabric Domain : "default"
Role : Edge
Control-Plane Service: Disabled
Number of "Control-Plane" node(s): 2
IP Address          Auth-key
-----
192.168.1.4         example-key1
192.168.1.5         example-key2

Number of "Border" node(s): 1
IP Address
-----
192.168.1.6

Number of context(s): 2
Codes: * - Not Configured

Name                ID      Host-pools
-----
default             0      *
example-context     10     1
```


show fabric context

```
show fabric context [{ default name }]
```

Syntax Description	default The default context
	name The name of a context in the fabric domain

Command Default Default context

Command Modes Privileged Exec

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the command to display a summary of the context configuration in your fabric domain.

```
device#show fabric context
Fabric-domain: default
Number of context(s): 2
  Name                ID          Host-pools
  -----
default              0          *
example-context      10         1
* - Not Configured
```

show fabric host-pool

show fabric host-pool*name*

Syntax Description	<i>name</i> The name of the host-pool
---------------------------	---------------------------------------

Command Default	None
------------------------	------

Command Modes	Privileged Exec
----------------------	-----------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	Use the command to display a summary of the specified host-pool configuration.
-------------------------	--

```

device# show fabric host-pool
Fabric Domain : "default"
context: default
  Number of host-pools : 0
  name                 vlan   prefix                gateway                use-dhcp
  -----
context: example-context
  Number of host-pools : 1
  name                 vlan   prefix                gateway                use-dhcp
  -----
VOICE_DOMAIN         10    192.168.1.0/24        192.168.1.254         209.65.201.6

```



PART II

Interface and Hardware Components

- [Interface and Hardware Commands, on page 29](#)



Interface and Hardware Commands

- [debug ilpower](#), on page 31
- [debug interface](#), on page 32
- [debug lldp packets](#), on page 33
- [debug platform poe](#), on page 34
- [duplex](#), on page 35
- [errdisable detect cause](#), on page 37
- [errdisable recovery cause](#), on page 39
- [errdisable recovery interval](#), on page 42
- [interface](#), on page 43
- [interface range](#), on page 45
- [ip mtu](#), on page 47
- [ipv6 mtu](#), on page 48
- [lldp \(interface configuration\)](#), on page 49
- [logging event power-inline-status](#), on page 51
- [mdix auto](#), on page 52
- [mode \(power-stack configuration\)](#), on page 53
- [network-policy](#), on page 55
- [network-policy profile \(global configuration\)](#), on page 56
- [power efficient-ethernet auto](#), on page 57
- [power-priority](#) , on page 58
- [power inline](#), on page 60
- [power inline police](#), on page 64
- [power supply](#), on page 66
- [show eee](#), on page 68
- [show env](#), on page 71
- [show errdisable detect](#), on page 74
- [show errdisable recovery](#), on page 75
- [show interfaces](#), on page 76
- [show interfaces counters](#), on page 80
- [show interfaces switchport](#), on page 82
- [show interfaces transceiver](#), on page 84
- [show memory platform](#), on page 87
- [show module](#), on page 90

- [show mgmt-infra trace messages ilpower](#), on page 91
- [show mgmt-infra trace messages ilpower-ha](#), on page 93
- [show mgmt-infra trace messages platform-mgr-poe](#), on page 94
- [show network-policy profile](#), on page 95
- [show platform hardware fed switch forward](#), on page 96
- [show platform resources](#), on page 98
- [show platform software ilpower](#), on page 99
- [show platform software process list](#), on page 101
- [show platform software process slot switch](#), on page 103
- [show platform software status control-processor](#), on page 105
- [show processes cpu platform monitor](#), on page 108
- [show processes memory platform](#), on page 110
- [show power inline](#), on page 113
- [show stack-power](#) , on page 119
- [show system mtu](#), on page 121
- [show tech-support](#) , on page 122
- [speed](#), on page 124
- [stack-power](#) , on page 126
- [switchport block](#), on page 128
- [system mtu](#), on page 129
- [test mcu read-register](#), on page 130
- [voice-signaling vlan \(network-policy configuration\)](#), on page 132
- [voice vlan \(network-policy configuration\)](#), on page 134

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** | **event** | **ha** | **ipc** | **police** | **port** | **powerman** | **registries** | **scp** | **sense** | **upoe**}
no debug ilpower {**cdp** | **event** | **ha** | **ipc** | **police** | **port** | **powerman** | **registries** | **scp** | **sense** | **upoe**}

Syntax Description

cdp	Displays PoE Cisco Discovery Protocol (CDP) 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 **undebg 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 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 undebg 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 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mbps.

Command Default

For Gigabit Ethernet ports, the default is **auto**.

For 100BASE-*x* (where *x* is -BX, -FX, -FX-FE, or -LX) SFP modules, the default is **half**.

Command Modes

Interface configuration (config-if)

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.

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.



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:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# duplex full
```

errdisable detect cause

To enable error-disable detection for a specific cause or for all causes, use the **errdisable detect cause** command in global configuration mode. To disable the error-disable detection feature, use the **no** form of this command.

```
errdisable detect cause {all | arp-inspection | bpduguard shutdown vlan | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | l2ptguard | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit |
security-violation shutdown vlan | sfp-config-mismatch}
no errdisable detect cause {all | arp-inspection | bpduguard shutdown vlan | dhcp-rate-limit | dtp-flap |
gbic-invalid | inline-power | l2ptguard | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit |
security-violation shutdown vlan | sfp-config-mismatch}
```

Syntax Description	
all	Enables error detection for all error-disabled causes.
arp-inspection	Enables error detection for dynamic Address Resolution Protocol (ARP) inspection.
bpduguard shutdown vlan	Enables per-VLAN error-disable for BPDU guard.
dhcp-rate-limit	Enables error detection for DHCP snooping.
dtp-flap	Enables error detection for the Dynamic Trunking Protocol (DTP) flapping.
gbic-invalid	Enables error detection for an invalid Gigabit Interface Converter (GBIC) module. Note This error refers to an invalid small form-factor pluggable (SFP) module.
inline-power	Enables error detection for the Power over Ethernet (PoE) error-disabled cause. Note This keyword is supported only on switches with PoE ports.
l2ptguard	Enables error detection for a Layer 2 protocol-tunnel error-disabled cause.
link-flap	Enables error detection for link-state flapping.
loopback	Enables error detection for detected loopbacks.
pagp-flap	Enables error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause.
pppoe-ia-rate-limit	Enables error detection for the PPPoE Intermediate Agent rate-limit error-disabled cause.
security-violation shutdown vlan	Enables voice aware 802.1x security.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.

Command Default Detection is enabled for all causes. All causes, except per-VLAN error disabling, are configured to shut down the entire port.

Command Modes Global configuration

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

Usage Guidelines A cause (such as a link-flap or dhcp-rate-limit) is the reason for the error-disabled state. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the bridge protocol data unit (BPDU) guard, voice-aware 802.1x security, and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

To verify your settings, enter the **show errdisable detect** privileged EXEC command.

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

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

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

```
Device(config)# errdisable detect cause bpduguard shutdown vlan
```

This command shows how to globally configure voice-aware 802.1x security for a per-VLAN error-disabled state:

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

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

errdisable recovery cause

To enable the error-disabled mechanism to recover from a specific cause, use the **errdisable recovery cause** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | l2ptguard | link-flap | loopback | mac-limit | pagp-flap |
port-mode-failure | pppoe-ia-rate-limit | psecure-violation | security-violation | sfp-config-mismatch |
storm-control | udld | vmps}
```

```
no errdisable recovery cause {all | arp-inspection | bpduguard | channel-misconfig | dhcp-rate-limit |
dtp-flap | gbic-invalid | inline-power | l2ptguard | link-flap | loopback | mac-limit | pagp-flap |
port-mode-failure | pppoe-ia-rate-limit | psecure-violation | security-violation | sfp-config-mismatch |
storm-control | udld | vmps}
```

Syntax Description

all	Enables the timer to recover from all error-disabled causes.
arp-inspection	Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.
bpduguard	Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.
channel-misconfig	Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.
dhcp-rate-limit	Enables the timer to recover from the DHCP snooping error-disabled state.
dtp-flap	Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.
gbic-invalid	Enables the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state. Note This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.
inline-power	Enables the timer to recover from the Power over Ethernet (PoE) error-disabled state. This keyword is supported only on switches with PoE ports.
l2ptguard	Enables the timer to recover from a Layer 2 protocol tunnel error-disabled state.
link-flap	Enables the timer to recover from the link-flap error-disabled state.
loopback	Enables the timer to recover from a loopback error-disabled state.
mac-limit	Enables the timer to recover from the mac limit error-disabled state.

pagp-flap	Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.
port-mode-failure	Enables the timer to recover from the port mode change failure error-disabled state.
pppoe-ia-rate-limit	Enables the timer to recover from the PPPoE IA rate limit error-disabled state.
psecure-violation	Enables the timer to recover from a port security violation disable state.
security-violation	Enables the timer to recover from an IEEE 802.1x-violation disabled state.
sfp-config-mismatch	Enables error detection on an SFP configuration mismatch.
storm-control	Enables the timer to recover from a storm control error.
udld	Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.
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 BPDU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down only the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you do not enable the recovery for the cause, the interface stays in the error-disabled state until you enter the **shutdown** and the **no shutdown** interface configuration commands. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

Examples

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


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

errdisable recovery interval

To specify the time to recover from an error-disabled state, use the **errdisable recovery interval** command in global configuration mode. To return to the default setting, use the **no** form of this command.

errdisable recovery interval *timer-interval*
no errdisable recovery interval *timer-interval*

Syntax Description	<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:

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

interface

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

```
interface {Auto-Template Auto-Template interface-number | GigabitEthernet Gigabit Ethernet interface number | Group VI Group VI interface number Internal Interface Internal Interface number Loopback Loopback interface number Null Null interface number Port-channel interface number Port-channel interface number TenGigabitEthernet interface number Tunnel interface number Vlan interface number }
```

Syntax	Description
Auto-Template <i>Auto-template interface-number</i>	Enables you to configure a auto-template interface. The range is 1 to 999.
GigabitEthernet <i>Gigabit Ethernet interface 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>Loopback Interface number</i>	Enables you to configure a loopback interface. The range is from 0 to 2147483647.
Null <i>Null 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>interface number</i>	Enables you to configure a 10-Gigabit Ethernet interface. The range is from 0 to 9.
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 0 to 4098.

Command Default None

Command Modes Global configuration

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

Usage Guidelines You can not use the "no" form of this command.

The following example shows how to configure a tunnel interface:

```
Device# interface Tunnel 15
```

interface range

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

interface range { **Auto-Template** *interface-number* | **GigabitEthernet** *switch-number/slot-number/port-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 an auto-template interface. The range is from 1 to 999.
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.
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.

interface range

Command Default None

Command Modes Global configuration

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

This example shows how you can configure interface range:

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

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:

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

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

```
Device(config)# interface vlan 200
Device(config-if)# default ip mtu
```

This is an example of partial output from the **show ip interface** *interface-id* command. It displays the current IP MTU setting for the interface.

```
Device# show ip interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
```

<output truncated>

ipv6 mtu

To set the IPv6 maximum transmission unit (MTU) size of routed packets on all routed ports of the switch or switch stack, use the **ipv6 mtu** command in interface configuration mode. To restore the default IPv6 MTU size, use the **no** form of this command.

ipv6 mtu *bytes*
no ipv6 mtu *bytes*

Syntax Description

bytes MTU size, in bytes. The range is from 1280 up to the system MTU value (in bytes).

Command Default

The default IPv6 MTU size for frames received and sent on all switch interfaces is 1500 bytes.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The upper limit of the IPv6 MTU value is based on the switch or switch stack configuration and refers to the currently applied system MTU value. For more information about setting the MTU sizes, see the **system mtu** global configuration command.

To return to the default IPv6 MTU setting, you can apply the **default ipv6 mtu** command or the **no ipv6 mtu** command on the interface.

You can verify your setting by entering the **show ipv6 interface** *interface-id* or **show interface** *interface-id* privileged EXEC command.

The following example sets the maximum IPv6 packet size for an interface to 2000 bytes:

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

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

```
Device(config)# interface gigabitethernet4/0/1
Device(config-if)# default ipv6 mtu
```

This is an example of partial output from the **show ipv6 interface** *interface-id* command. It displays the current IPv6 MTU setting for the interface.

```
Device# show ipv6 interface gigabitethernet4/0/1
GigabitEthernet4/0/1 is up, line protocol is up
  Internet address is 18.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
```

<output truncated>

lldp (interface configuration)

To enable Link Layer Discovery Protocol (LLDP) on an interface, use the **lldp** command in interface configuration mode. To disable LLDP on an interface, use the **no** form of this command.

```
lldp {med-tlv-select tlv | receive | tlv-select power-management | transmit}
no lldp {med-tlv-select tlv | receive | tlv-select power-management | transmit}
```

Syntax Description		
med-tlv-select		Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.
<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:

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

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

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

```
Device(config-if)# lldp transmit
```

logging event power-inline-status

To enable the logging of Power over Ethernet (PoE) events, use the **logging event power-inline-status** command in interface configuration mode. To disable the logging of PoE status events, use the **no** form of this command.

logging event power-inline-status
no logging event power-inline-status

Syntax Description This command has no arguments or keywords.

Command Default Logging of PoE events is enabled.

Command Modes Interface configuration

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

Usage Guidelines The **no** form of this command does not disable PoE error events.

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

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

mdix auto

To enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface, use the **mdix auto** command in interface configuration mode. To disable auto-MDIX, use the **no** form of this command.

mdix auto
no mdix auto

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	Auto-MDIX is enabled.
------------------------	-----------------------

Command Modes	Interface configuration
----------------------	-------------------------

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

Usage Guidelines	When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately.
-------------------------	--

When you enable auto-MDIX on an interface, you must also set the interface speed and duplex to **auto** so that the feature operates correctly.

When auto-MDIX (and autonegotiation of speed and duplex) is enabled on one or both of the connected interfaces, link up occurs, even if the cable type (straight-through or crossover) is incorrect.

This example shows how to enable auto-MDIX on a port:

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

mode (power-stack configuration)

To configure power stack mode for the power stack, use the **mode** command in power-stack configuration mode. To return to the default settings, use the **no** form of the command.

mode {**power-shared** | **redundant**} [**strict**]
no mode

Syntax Description		
power-shared	Sets the power stack to operate in power-shared mode. This is the default.	
redundant	Sets the power stack to operate in redundant mode. The largest power supply is removed from the power pool to be used as backup power in case one of the other power supplies fails.	
strict	(Optional) Configures the power stack mode to run a strict power budget. The stack power needs cannot exceed the available power.	

Command Default The default modes are **power-shared** and nonstrict.

Command Modes Power-stack configuration

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

Usage Guidelines This command is available only on switch stacks running the IP Base or IP Services feature set. To access power-stack configuration mode, enter the **stack-power stack** *power stack name* global configuration command.

Entering the **no mode** command sets the switch to the defaults of **power-shared** and non-strict mode.



Note For stack power, available power is the total power available for PoE from all power supplies in the power stack, available power is the power allocated to all powered devices connected to PoE ports in the stack, and consumed power is the actual power consumed by the powered devices.

In **power-shared** mode, all of the input power can be used for loads, and the total available power appears as one large power supply. The power budget includes all power from all supplies. No power is set aside for power supply failures. If a power supply fails, load shedding (shutting down of powered devices or switches) might occur.

In **redundant** mode, the largest power supply is removed from the power pool to use as backup power in case one of the other power supplies fails. The available power budget is the total power minus the largest power supply. This reduces the available power in the pool for switches and powered devices, but in case of a failure or an extreme power load, there is less chance of having to shut down switches or powered devices.

In **strict** mode, when a power supply fails and the available power drops below the budgeted power, the system balances the budget through load shedding of powered devices, even if the actual power is less than the available power. In nonstrict mode, the power stack can run in an over-allocated state and is stable as long as

the actual power does not exceed the available power. In this mode, a powered device drawing more than normal power could cause the power stack to start shedding loads. This is normally not a problem because most devices do not run at full power. The chances of multiple powered devices in the stack requiring maximum power at the same time is small.

In both strict and nonstrict modes, power is denied when there is no power available in the power budget.

This is an example of setting the power stack mode for the stack named power1 to power-shared with strict power budgeting. All power in the stack is shared, but when the total available power is allotted, no more devices are allowed power.

```
Device(config)# stack-power stack power1  
Device(config-stackpower)# mode power-shared strict  
Device(config-stackpower)# exit
```

This is an example of setting the power stack mode for the stack named power2 to redundant. The largest power supply in the stack is removed from the power pool to provide redundancy in case one of the other supplies fails.

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

network-policy

To apply a network-policy profile to an interface, use the **network-policy** command in interface configuration mode. To remove the policy, use the **no** form of this command.

```
network-policy profile-number
no network-policy
```

Syntax Description

profile-number The network-policy profile number to apply to the interface.

Command Default

No network-policy profiles are applied.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **network-policy** *profile number* interface configuration command to apply a profile to an interface.

You cannot apply the **switchport voice vlan** command on an interface if you first configure a network-policy profile on it. However, if **switchport voice vlan** *vlan-id* is already configured on the interface, you can apply a network-policy profile on the interface. The interface then has the voice or voice-signaling VLAN network-policy profile applied.

This example shows how to apply network-policy profile 60 to an interface:

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

network-policy profile (global configuration)

To create a network-policy profile and to enter network-policy configuration mode, use the **network-policy profile** command in global configuration mode. To delete the policy and to return to global configuration mode, use the **no** form of this command.

network-policy profile *profile-number*
no network-policy profile *profile-number*

Syntax Description	<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	<p>Use the network-policy profile global configuration command to create a profile and to enter network-policy profile configuration mode.</p> <p>To return to privileged EXEC mode from the network-policy profile configuration mode, enter the exit command.</p> <p>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.</p> <p>These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).</p> <p>This example shows how to create network-policy profile 60:</p> <pre>Device(config)# network-policy profile 60 Device(config-network-policy)#</pre>	

power efficient-ethernet auto

To enable Energy Efficient Ethernet (EEE) for an interface, use the **power efficient-ethernet auto** command in interface configuration mode. To disable EEE on an interface, use the **no** form of this command.

power efficient-ethernet auto
no power efficient-ethernet auto

Syntax Description This command has no arguments or keywords.

Command Default EEE is disabled.

Command Modes Interface configuration

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

Usage Guidelines You can enable EEE on devices that support low power idle (LPI) mode. Such devices can save power by entering LPI mode during periods of low utilization. In LPI mode, systems on both ends of the link can save power by shutting down certain services. EEE provides the protocol needed to transition into and out of LPI mode in a way that is transparent to upper layer protocols and applications.

The **power efficient-ethernet auto** command is available only if the interface is EEE capable. To check if an interface is EEE capable, use the **show eee capabilities EXEC** command.

When EEE is enabled, the device advertises and autonegotiates EEE to its link partner. To view the current EEE status for an interface, use the **show eee status EXEC** command.

This command does not require a license.

This example shows how to enable EEE for an interface:

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

This example shows how to disable EEE for an interface:

```
Device(config-if) # no power efficient-ethernet auto
Device(config-if) #
```

power-priority

To configure Cisco StackPower power-priority values for a switch in a power stack and for its high-priority and low-priority PoE ports, use the **power-priority** command in switch stack-power configuration mode. To return to the default setting, use the **no** form of the command.

```
power-priority {high value | low value | switch value}
no power-priority {high | low | switch}
```

Syntax Description

high <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.

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

power inline

To configure the power management mode on Power over Ethernet (PoE) ports, use the **power inline** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
power inline {auto [max max-wattage] | four-pair forced | never | port priority {high | low} | static [max max-wattage]}
no power inline {auto | four-pair forced | never | port priority {high | low} | static [max max-wattage]}
```

Syntax Description

auto	Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. Allocation is first-come, first-serve.
max <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:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline auto
                        ^
% Invalid input detected at '^' marker.
```

In a switch stack, this command is supported on all ports in the stack that support PoE.

Cisco Universal Power Over Ethernet (Cisco UPOE) is a Cisco proprietary technology that extends the IEEE 802.3at 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:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto
```

This example shows how to automatically enable power on both signal and spare pairs from switch port Gigabit Ethernet 1/0/1:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# power inline four-pair forced
```

This example shows how to configure a PoE port on a switch to allow a class 1 or a class 2 powered device:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline auto max 7000
```

This example shows how to disable powered-device detection and to not power a PoE port on a switch:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# power inline never
```

This example shows how to set the priority of a port to high, so that it would be one of the last ports to be shut down in case of power supply failure:

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

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

power inline police

To enable policing of real-time power consumption on a powered device, use the **power inline police** command in interface configuration mode. To disable this feature, use the **no** form of this command

```
power inline police [action {errdisable | log}]
no power inline police
```

Syntax Description

action errdisable	(Optional) Configures the device to turn off power to the port if the real-time power consumption exceeds the maximum power allocation on the port. This is the default action.
action log	(Optional) Configures the device to generate a syslog message while still providing power to a connected device if the real-time power consumption exceeds the maximum power allocation on the port.

Command Default

Policing of the real-time power consumption of the powered device is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

This command is supported only on the LAN Base image.

This command is supported only on Power over Ethernet (PoE)-capable ports. If you enter this command on a device or port that does not support PoE, an error message appears.

In a switch stack, this command is supported on all switches or ports in the stack that support PoE and real-time power-consumption monitoring.

When policing of the real-time power consumption is enabled, the device takes action when a powered device consumes more power than the allocated maximum amount.

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

When power policing is enabled, the device uses one of the these values as the cutoff power on the PoE port in this order:

1. The user-defined power level that limits the power allowed on the port when you enter the **power inline auto max** *max-wattage* or the **power inline static max** *max-wattage* interface configuration command
2. The device automatically sets the power usage of the device by using CDP power negotiation or by the IEEE classification and LLDP power negotiation.

If you do not manually configure the cutoff-power value, the device automatically determines it by using CDP power negotiation or the device IEEE classification and LLDP power negotiation. If CDP or LLDP are not enabled, the default value of 30 W is applied. However without CDP or LLDP, the device does not allow devices to consume more than 15.4 W of power because values from 15400 to 30000 mW are only allocated based on CDP or LLDP requests. If a powered device consumes more than 15.4 W without CDP or LLDP

negotiation, the device might be in violation of the maximum current 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 device locks to the power-negotiation protocol of that first packet and does not respond to power requests from the other protocol. For example, if the device is locked to CDP, it does not provide power to devices that send LLDP requests. If CDP is disabled after the device has locked on it, the device does not respond to LLDP power requests and can no longer power on any accessories. In this case, you should restart the powered device.

If power policing is enabled, the device polices power usage by comparing the real-time power consumption to the maximum power allocated on the PoE port. If the device uses more than the maximum power allocation (or *cutoff power*) on the port, the device either turns power off to the port, or the device generates a syslog message and updates the LEDs (the port LEDs are blinking amber) while still providing power to the device.

- To configure the device to turn off power to the port and put the port in the error-disabled state, use the **power inline police** interface configuration command.
- To configure the device to generate a syslog message while still providing power to the device, use the **power inline police action log** command.

If you do not enter the **action log** keywords, the default action is to shut down the port, turn off power to it, and put the port in the PoE error-disabled state. To configure the PoE port to automatically recover from the error-disabled state, use the **errdisable detect cause inline-power** global configuration command to enable error-disabled detection for the PoE cause and the **errdisable recovery cause inline-power interval interval** global configuration command to enable the recovery timer for the PoE error-disabled cause.



Caution

If policing is disabled, no action occurs when the powered device consumes more than the maximum power allocation on the port, which could adversely affect the device.

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

Examples

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

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

power supply

To configure and manage the internal power supplies on a switch, use the **power supply** command in privileged EXEC mode.

power supply *stack-member-number* **slot** {**A** | **B**} {**off** | **on**}

Syntax Description		
<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:

```
Device> power supply 2 slot A off
Disabling Power supply A may result in a power loss to PoE devices and/or switches ...
Continue? (yes/[no]): yes
Device
```

```
Jun 10 04:52:54.389: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered off
Jun 10 04:52:56.717: %PLATFORM_ENV-1-FAN_NOT_PRESENT: Fan is not present
```

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

```
Device> power supply 1 slot B on
Jun 10 04:54:39.600: %PLATFORM_ENV-6-FRU_PS_OIR: FRU Power Supply 1 powered on
```

This example shows the output of the show env power command:

```
Device> show env power
SW  PID                Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  PWR-1RUC2-640WAC    DCB1705B05B OK           Good     Good     250/390
1B  Not Present
```

show 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:

```
Device# show eee capabilities interface gigabitethernet1/0/1
Gi1/0/1
    EEE(efficient-ethernet):  yes (100-Tx and 1000T auto)
    Link Partner              :  yes (100-Tx and 1000T auto)
```

This is an example of output from the **show eee capabilities** command on an interface where EEE is not enabled:

```
Device# show eee capabilities interface gigabitethernet2/0/1
Gi2/0/1
    EEE(efficient-ethernet):  not enabled
```

```
Link Partner          : not enabled
```

This is an example of output from the **show eee status** command on an interface where EEE is enabled and operational. The table that follows describes the fields in the display.

```
Device# show eee status interface gigabitethernet1/0/4
Gi1/0/4 is up
  EEE(efficient-ethernet): Operational
  Rx LPI Status           : Received
  Tx LPI Status           : Received
```

This is an example of output from the **show eee status** command on an interface where EEE is operational and the ports are in low power save mode:

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is up
  EEE(efficient-ethernet): Operational
  Rx LPI Status           : Low Power
  Tx LPI Status           : Low Power
  Wake Error Count        : 0
```

This is an example of output from the **show eee status** command on an interface where EEE is not enabled because a remote link partner is incompatible with EEE:

```
Device# show eee status interface gigabitethernet1/0/3
Gi1/0/3 is down
  EEE(efficient-ethernet): Disagreed
  Rx LPI Status           : None
  Tx LPI Status           : None
  Wake Error Count        : 0
```

Table 6: 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

This is an example of output from the **show env all** command:

```
Device>show env all
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC             LIT150119Z1 OK            Good      Good     715
```

This is an example of output from the **show env fan** command:

```
Device>show env fan
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
```

This is an example of output from the **show env power** command:

```
Device>show env power
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC             LIT150119Z1 OK            Good      Good     715
```

This is an example of output from the **show env power all** command on the active switch:

```
Device# show env power all
SW  PID                      Serial#      Status          Sys Pwr  PoE Pwr  Watts
--  -
1A  Not Present
1B  PWR-C1-715WAC             LIT150119Z1 OK            Good      Good     715
```

This is an example of output from the **show env stack** command on the active switch:

```
Device> show env stack
SWITCH: 1
Switch 1 FAN 1 is OK
Switch 1 FAN 2 is OK
Switch 1 FAN 3 is OK
FAN PS-1 is NOT PRESENT
FAN PS-2 is OK
Switch 1: SYSTEM TEMPERATURE is OK
```



```
Temperature Value: 28 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold    : 56 Degree Celsius
```

This example shows how to display the temperature value, state, and the threshold values on a standalone switch. The table describes the temperature states in the command output.

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

Table 7: 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.

```
Device> show errdisable detect
ErrDisable Reason    Detection    Mode
-----
arp-inspection       Enabled     port
bpduguard            Enabled     vlan
channel-misconfig    Enabled     port
community-limit      Enabled     port
dhcp-rate-limit      Enabled     port
dtp-flap             Enabled     port
gbic-invalid         Enabled     port
inline-power         Enabled     port
invalid-policy       Enabled     port
l2ptguard           Enabled     port
link-flap            Enabled     port
loopback             Enabled     port
lsgroup              Enabled     port
pagp-flap            Enabled     port
psecure-violation    Enabled     port/vlan
security-violatio    Enabled     port
sfp-config-mismat    Enabled     port
storm-control        Enabled     port
udld                 Enabled     port
```

show errdisable recovery

To display the error-disabled recovery timer information, use the **show errdisable recovery** command in EXEC mode.

show errdisable recovery

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines A gbic-invalid error-disable reason refers to an invalid small form-factor pluggable (SFP) module interface.



Note Though visible in the output, the unicast-flood field is not valid.

This is an example of output from the **show errdisable recovery** command:

```
Device> show errdisable recovery
ErrDisable Reason      Timer Status
-----
udld                    Disabled
bpduguard              Disabled
security-violatio     Disabled
channel-misconfig     Disabled
pagg-flap              Disabled
dtp-flap               Disabled
link-flap              Enabled
l2ptguard              Disabled
psecure-violation     Disabled
gbic-invalid           Disabled
dhcp-rate-limit       Disabled
unicast-flood         Disabled
storm-control         Disabled
arp-inspection        Disabled
loopback               Disabled
Timer interval:300 seconds
Interfaces that will be enabled at the next timeout:
Interface      Errdisable reason      Time left(sec)
-----
Gi1/0/2        link-flap                279
```

show interfaces

To display the administrative and operational status of all interfaces or for a specified interface, use the **show interfaces** command in privileged EXEC mode.

```
show interfaces [{interface-id|vlan vlan-id}] [{accounting|capabilities [module number]|debounce
|description|etherchannel|flowcontrol|pruning|stats|status [{err-disabled|inactive}]|trunk}]
```

Syntax Description

<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:

```
Device# show interfaces gigabitethernet3/0/2
GigabitEthernet3/0/2 is down, line protocol is down (notconnect)
  Hardware is Gigabit Ethernet, address is 2037.064d.4381 (bia 2037.064d.4381)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```

0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts (0 multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out

```

Device# **show interfaces gigabitethernet1/0/2 capabilities**

```

GigabitEthernet1/0/2
  Model:                UA-3850-24-CR
  Type:                 10/100/1000BaseTX
  Speed:               10,100,1000,auto
  Duplex:              full,half,auto
  Trunk encap. type:   802.1Q
  Trunk mode:         on,off,desirable,nonegotiate
  Channel:             yes
  Fast Start:         yes
  QoS scheduling:     rx-(not configurable on per port basis),
                    tx-(4q3t) (3t: Two configurable values and one fixed.)
  CoS rewrite:        yes
  ToS rewrite:        yes
  UDL:                 yes
  Inline power:       no
  SPAN:               source/destination
  PortSecure:         yes
  Dot1x:              yes

```

This is an example of output from the **show interfaces interface description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command:

Device# **show interfaces gigabitethernet1/0/2 description**

```

Interface          Status      Protocol Description
Gi1/0/2            up          down      Connects to Marketing

```

This is an example of output from the **show interfaces interface-id pruning** command when pruning is enabled in the VTP domain:

```

Device# show interfaces gigabitethernet1/0/2 pruning
Port      Vlans pruned for lack of request by neighbor
Gi1/0/2   3,4

Port      Vlans traffic requested of neighbor
Gi1/0/2   1-3

```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface:

```

Device# show interfaces vlan 1 stats
Switching path  Pkts In   Chars In   Pkts Out   Chars Out
  Processor    1165354   136205310   570800     91731594
  Route cache      0         0           0           0
  Total        1165354   136205310   570800     91731594

```

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

```
Device# show interfaces gigabitethernet1/0/20 status
Port      Name              Status      Vlan      Duplex  Speed      Type
Gi1/0/20              notconnect  1          auto     auto    10/100/1000Ba
seTX
```

This is an example of output from the **show interfaces status err-disabled** command. It displays the status of interfaces in the error-disabled state:

```
Device# show interfaces status err-disabled
Port      Name              Status      Reason
Gi1/0/2   err-disabled     gbic-invalid
Gi2/0/3   err-disabled     dtp-flap
```

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

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

```
Device# show interfaces gigabitethernet1/0/1 trunk
Port      Mode              Encapsulation  Status      Native vlan
Gi1/0/1   on                802.1q         other       10

Port      Vlans allowed on trunk
Gi1/0/1   none

Port      Vlans allowed and active in management domain
Gi1/0/1   none

Port      Vlans in spanning tree forwarding state and not pruned
Gi1/0/1   none
```

show interfaces counters

To display various counters for the switch or for a specific interface, use the **show interfaces counters** command in privileged EXEC mode.

show interfaces [*interface-id*] **counters** [{**errors** | **etherchannel** | **module** *stack-member-number* | **protocol status** | **trunk**}]

Syntax Description		
<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.

```
Device# show interfaces counters
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/0/1             0             0             0             0
Gi1/0/2             0             0             0             0
Gi1/0/3      95285341     43115         1178430       1950
Gi1/0/4             0             0             0             0
```


<output truncated>

This is an example of partial output from the **show interfaces counters module** command for stack member 2. It displays all counters for the specified switch in the stack.

```
Device# show interfaces counters module 2
Port          InOctets    InUcastPkts  InMcastPkts  InBcastPkts
Gi1/0/1       520         2            0            0
Gi1/0/2       520         2            0            0
Gi1/0/3       520         2            0            0
Gi1/0/4       520         2            0            0
```

<output truncated>

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces:

```
Device# show interfaces counters protocol status
Protocols allocated:
Vlan1: Other, IP
Vlan20: Other, IP, ARP
Vlan30: Other, IP, ARP
Vlan40: Other, IP, ARP
Vlan50: Other, IP, ARP
Vlan60: Other, IP, ARP
Vlan70: Other, IP, ARP
Vlan80: Other, IP, ARP
Vlan90: Other, IP, ARP
Vlan900: Other, IP, ARP
Vlan3000: Other, IP
Vlan3500: Other, IP
GigabitEthernet1/0/1: Other, IP, ARP, CDP
GigabitEthernet1/0/2: Other, IP
GigabitEthernet1/0/3: Other, IP
GigabitEthernet1/0/4: Other, IP
GigabitEthernet1/0/5: Other, IP
GigabitEthernet1/0/6: Other, IP
GigabitEthernet1/0/7: Other, IP
GigabitEthernet1/0/8: Other, IP
GigabitEthernet1/0/9: Other, IP
GigabitEthernet1/0/10: Other, IP, CDP
```

<output truncated>

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Device# show interfaces counters trunk
Port          TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi1/0/1       0              0              0
Gi1/0/2       0              0              0
Gi1/0/3       80678         0              0
Gi1/0/4       82320         0              0
Gi1/0/5       0              0              0
```

<output truncated>

show interfaces switchport

To display the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings, use the **show interfaces switchport** command in privileged EXEC mode.

show interfaces [*interface-id*] **switchport** [{**module number**}]

Syntax Description	<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.				
	module number (Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. The range is 1 to 9. This option is not available if you entered a specific interface ID.				
Command Default	None				
Command Modes	Privileged EXEC				
Command History	<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 Use the **show interface switchport module number** command to display the switch port characteristics of all interfaces on that switch in the stack. If there is no switch with that module number in the stack, there is no output.

This is an example of output from the **show interfaces switchport** command for a port. The table that follows describes the fields in the display.



Note Private VLANs are not supported in this release, so those fields are not applicable.

```
Device# show interfaces gigabitethernet1/0/1 switchport
Name: Gi1/0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 10 (VLAN0010)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
```

```

Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: 11-20
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

```

```

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

```

Field	Description
Name	Displays the port name.
Switchport	Displays the administrative and operational status of the port. In this display, the port is in switchport mode.
Administrative Mode Operational Mode	Displays the administrative and operational modes.
Administrative Trunking Encapsulation Operational Trunking Encapsulation Negotiation of Trunking	Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled.
Access Mode VLAN	Displays the VLAN ID to which the port is configured.
Trunking Native Mode VLAN Trunking VLANs Enabled Trunking VLANs Active	Lists the VLAN ID of the trunk that is in native mode. Lists the allowed VLANs on the trunk. Lists the active VLANs on the trunk.
Pruning VLANs Enabled	Lists the VLANs that are pruning-eligible.
Protected	Displays whether or not protected port is enabled (True) or disabled (False) on the interface.
Unknown unicast blocked Unknown multicast blocked	Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface.
Voice VLAN	Displays the VLAN ID on which voice VLAN is enabled.
Appliance trust	Displays the class of service (CoS) setting of the data packets of the IP phone.

show interfaces transceiver

To display the physical properties of a small form-factor pluggable (SFP) module interface, use the **show interfaces transceiver** command in EXEC mode.

show interfaces [*interface-id*] **transceiver** [{**detail** | **module number** | **properties** | **supported-list** | **threshold-table**}]

Syntax Description	
<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 number	(Optional) Limits display to interfaces on module on the switch. The range is 1 to 9. This option is not available if you entered a specific interface ID.
properties	(Optional) Displays speed, duplex, and inline power settings on an interface.
supported-list	(Optional) Lists all supported transceivers.
threshold-table	(Optional) Displays alarm and warning threshold table.

Command Modes	
	User EXEC
	Privileged EXEC

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

Examples

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

```
Device# show interfaces gigabitethernet1/1/1 transceiver properties
Name : Gi1/1/1
Administrative Speed: auto
Operational Speed: auto
Administrative Duplex: auto
Administrative Power Inline: enable
Operational Duplex: auto
Administrative Auto-MDIX: off
Operational Auto-MDIX: off
```

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

```
Device# show interfaces gigabitethernet1/1/1 transceiver detail
ITU Channel not available (Wavelength not available),
```

Transceiver is internally calibrated.
 mA:milliamperes, dBm:decibels (milliwatts), N/A:not applicable.
 ++:high alarm, +:high warning, -:low warning, -- :low alarm.
 A2D readouts (if they differ), are reported in parentheses.
 The threshold values are uncalibrated.

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

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

```
Device# show interfaces transceiver threshold-table
```

	Optical Tx	Optical Rx	Temp	Laser Bias current	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
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

show interfaces transceiver

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
CWD M X2					
Min1	N/A	N/A	0	N/A	N/A
Min2	N/A	N/A	0	N/A	N/A
Max2	N/A	N/A	0	N/A	N/A
Max1	N/A	N/A	0	N/A	N/A

<output truncated>

show memory platform

To display memory statistics of a platform, use the **show memory platform** command in privileged EXEC mode.

```
show memory platform [{compressed-swap | information | page-merging}]
```

Syntax Description	
compressed-swap	(Optional) Displays platform memory compressed-swap information.
information	(Optional) Displays general information about the platform.
page-merging	(Optional) Displays platform memory page-merging information.

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines	Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.
------------------	--

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show memory platform** command:

```
Switch# show memory platform

Virtual memory   : 12874653696
Pages resident  : 627041
Major page faults: 2220
Minor page faults: 2348631

Architecture    : mips64
Memory (kB)
  Physical       : 3976852
  Total          : 3976852
  Used           : 2761276
  Free           : 1215576
  Active         : 2128196
  Inactive       : 1581856
  Inact-dirty    : 0
  Inact-clean    : 0
  Dirty          : 0
  AnonPages     : 1294984
  Bounce         : 0
  Cached         : 1978168
  Commit Limit  : 1988424
  Committed As  : 3343324
  High Total    : 0
  High Free     : 0
  Low Total     : 3976852
  Low Free      : 1215576
```

show memory platform

```

Mapped          : 516316
NFS Unstable    : 0
Page Tables     : 17124
Slab            : 0
VMmalloc Chunk  : 1069542588
VMmalloc Total  : 1069547512
VMmalloc Used   : 2588
Writeback       : 0
HugePages Total: 0
HugePages Free  : 0
HugePages Rsvd  : 0
HugePage Size   : 2048

Swap (kB)
Total           : 0
Used            : 0
Free            : 0
Cached         : 0

Buffers (kB)    : 437136

Load Average
1-Min          : 1.04
5-Min          : 1.16
15-Min         : 0.94

```

The following is sample output from the **show memory platform information** command:

Device# **show memory platform information**

```

Virtual memory   : 12870438912
Pages resident   : 626833
Major page faults: 2222
Minor page faults: 2362455

Architecture     : mips64
Memory (kB)
Physical         : 3976852
Total           : 3976852
Used            : 2761224
Free            : 1215628
Active          : 2128060
Inactive        : 1584444
Inact-dirty     : 0
Inact-clean     : 0
Dirty           : 284
AnonPages       : 1294656
Bounce          : 0
Cached          : 1979644
Commit Limit    : 1988424
Committed As    : 3342184
High Total      : 0
High Free       : 0
Low Total       : 3976852
Low Free        : 1215628
Mapped          : 516212
NFS Unstable    : 0
Page Tables     : 17096
Slab            : 0
VMmalloc Chunk  : 1069542588
VMmalloc Total  : 1069547512
VMmalloc Used   : 2588
Writeback       : 0

```



```
HugePages Total: 0
HugePages Free : 0
HugePages Rsvd : 0
HugePage Size  : 2048

Swap (kB)
  Total      : 0
  Used       : 0
  Free       : 0
  Cached     : 0

Buffers (kB) : 438228

Load Average
  1-Min      : 1.54
  5-Min      : 1.27
  15-Min     : 0.99
```

show module

To display module information such as switch number, model number, serial number, hardware revision number, software version, MAC address and so on, use this command in user EXEC or privileged EXEC mode.

```
show module [{switch-num}]
```

Syntax Description	<i>switch-num</i>	(Optional) Number of the switch.
Command Default	None	
Command Modes	User EXEC (>) Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.
Usage Guidelines	Entering the show module command without the <i>switch-num</i> argument is the same as entering the show module all command.	
Examples	This example shows how to display information for all the modules on a Cisco Catalyst 3850 Series switch:	

show mgmt-infra trace messages ilpower

To display inline power messages within a trace buffer, use the **show mgmt-infra trace messages ilpower** command in privileged EXEC mode.

show mgmt-infra trace messages ilpower [**switch** *stack-member-number*]

Syntax Description	switch <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:

```
Device# show mgmt-infra trace messages ilpower
[10/23/12 14:05:10.984 UTC 1 3] Initialized inline power system configuration fo
r slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration fo
r slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration fo
r slot 3.
[10/23/12 14:05:10.984 UTC 4 3] Initialized inline power system configuration fo
r slot 4.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration fo
r slot 5.
[10/23/12 14:05:10.984 UTC 6 3] Initialized inline power system configuration fo
r slot 6.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration fo
r slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration fo
r slot 8.
[10/23/12 14:05:10.984 UTC 9 3] Initialized inline power system configuration fo
r slot 9.
[10/23/12 14:05:10.984 UTC a 3] Inline power subsystem initialized.
[10/23/12 14:05:18.908 UTC b 264] Create new power pool for slot 1
[10/23/12 14:05:18.909 UTC c 264] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.273 UTC d 3] PoE is not supported on .
[10/23/12 14:05:20.288 UTC e 3] PoE is not supported on .
[10/23/12 14:05:20.299 UTC f 3] PoE is not supported on .
[10/23/12 14:05:20.311 UTC 10 3] PoE is not supported on .
[10/23/12 14:05:20.373 UTC 11 98] Inline power process post for switch 1
[10/23/12 14:05:20.373 UTC 12 98] PoE post passed on switch 1
[10/23/12 14:05:20.379 UTC 13 3] Slot #1: PoE initialization for board id 16387
[10/23/12 14:05:20.379 UTC 14 3] Set total inline power to 450 for slot 1
[10/23/12 14:05:20.379 UTC 15 3] Gi1/0/1 port config Initialized
[10/23/12 14:05:20.379 UTC 16 3] Interface Gi1/0/1 initialization done.
[10/23/12 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
[10/23/12 14:05:20.380 UTC 18 3] Interface Gi1/0/24 initialization done.
[10/23/12 14:05:20.380 UTC 19 3] Slot #1: initialization done.
```

```
show mgmt-infra trace messages ilpower
```

```
[10/23/12 14:05:50.440 UTC 1a 3] Slot #1: PoE initialization for board id 16387  
[10/23/12 14:05:50.440 UTC 1b 3] Duplicate init event
```

show mgmt-infra trace messages ilpower-ha

To display inline power high availability messages within a trace buffer, use the **show mgmt-infra trace messages ilpower-ha** command in privileged EXEC mode.

```
show mgmt-infra trace messages ilpower-ha [switch stack-member-number]
```

Syntax Description	switch <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:

```
Device# show mgmt-infra trace messages ilpower-ha
[10/23/12 14:04:48.087 UTC 1 3] NG3K_ILPOWER_HA: Created NGWC ILP CF client successfully.
```

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:

```
Device# show mgmt-infra trace messages platform-mgr-poe
[10/23/12 14:04:06.431 UTC 1 5495] PoE Info: get power controller param sent:
[10/23/12 14:04:06.431 UTC 2 5495] PoE Info: POE_SHUT sent for port 1 (0:0)
[10/23/12 14:04:06.431 UTC 3 5495] PoE Info: POE_SHUT sent for port 2 (0:1)
[10/23/12 14:04:06.431 UTC 4 5495] PoE Info: POE_SHUT sent for port 3 (0:2)
[10/23/12 14:04:06.431 UTC 5 5495] PoE Info: POE_SHUT sent for port 4 (0:3)
[10/23/12 14:04:06.431 UTC 6 5495] PoE Info: POE_SHUT sent for port 5 (0:4)
[10/23/12 14:04:06.431 UTC 7 5495] PoE Info: POE_SHUT sent for port 6 (0:5)
[10/23/12 14:04:06.431 UTC 8 5495] PoE Info: POE_SHUT sent for port 7 (0:6)
[10/23/12 14:04:06.431 UTC 9 5495] PoE Info: POE_SHUT sent for port 8 (0:7)
[10/23/12 14:04:06.431 UTC a 5495] PoE Info: POE_SHUT sent for port 9 (0:8)
[10/23/12 14:04:06.431 UTC b 5495] PoE Info: POE_SHUT sent for port 10 (0:9)
[10/23/12 14:04:06.431 UTC c 5495] PoE Info: POE_SHUT sent for port 11 (0:10)
[10/23/12 14:04:06.431 UTC d 5495] PoE Info: POE_SHUT sent for port 12 (0:11)
[10/23/12 14:04:06.431 UTC e 5495] PoE Info: POE_SHUT sent for port 13 (e:0)
[10/23/12 14:04:06.431 UTC f 5495] PoE Info: POE_SHUT sent for port 14 (e:1)
[10/23/12 14:04:06.431 UTC 10 5495] PoE Info: POE_SHUT sent for port 15 (e:2)
[10/23/12 14:04:06.431 UTC 11 5495] PoE Info: POE_SHUT sent for port 16 (e:3)
[10/23/12 14:04:06.431 UTC 12 5495] PoE Info: POE_SHUT sent for port 17 (e:4)
[10/23/12 14:04:06.431 UTC 13 5495] PoE Info: POE_SHUT sent for port 18 (e:5)
[10/23/12 14:04:06.431 UTC 14 5495] PoE Info: POE_SHUT sent for port 19 (e:6)
[10/23/12 14:04:06.431 UTC 15 5495] PoE Info: POE_SHUT sent for port 20 (e:7)
[10/23/12 14:04:06.431 UTC 16 5495] PoE Info: POE_SHUT sent for port 21 (e:8)
[10/23/12 14:04:06.431 UTC 17 5495] PoE Info: POE_SHUT sent for port 22 (e:9)
[10/23/12 14:04:06.431 UTC 18 5495] PoE Info: POE_SHUT sent for port 23 (e:10)
```

show network-policy profile

To display the network-policy profiles, use the **show network policy profile** command in privileged EXEC mode.

show network-policy profile [*profile-number*]

Syntax Description	<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:

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

show platform hardware fed switch forward

To display device-specific hardware information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the forwarding-specific options, that is, the options available with the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** command.

The output of the **show platform hardware fed switch** *switch_number* **forward summary** displays all the details about the forwarding decision taken for the packet.

show platform hardware fed switch {*switch_num* | **active** | **standby**} **forward summary**

Syntax Description	<p>switch {<i>switch_num</i> active standby }</p> <p>The switch for which you want to display information. You have the following options :</p> <ul style="list-style-type: none"> • <i>switch_num</i>—ID of the switch. • active—Displays information relating to the active switch. • standby—Displays information relating to the standby switch, if available.
	<p>forward summary Displays packet forwarding information.</p>

Command Modes Privileged EXEC

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

Usage Guidelines Do not use this command unless a technical support representative asks you to. Use this command only when you are working directly with a technical support representative while troubleshooting a problem.

Fields displayed in the command output are explained below.

- **Station Index** : The Station Index is the result of the layer 2 lookup and points to a station descriptor which provides the following:
 - **Destination Index** : Determines the egress port(s) to which the packets should be sent to. Global Port Number(GPN) can be used as the destination index. A destination index with 15 down to 12 bits set indicates the GPN to be used. For example, destination index - 0xF04E corresponds to GPN - 78 (0x4e).
 - **Rewrite Index** : Determines what needs to be done with the packets. For layer 2 switching, this is typically a bridging action
 - **Flexible Lookup Pipeline Stages(FPS)** : Indicates the forwarding decision that was taken for the packet - routing or bridging
 - **Replication Bit Map** : Determines if the packets should be sent to CPU or stack
 - Local Data Copy = 1

- Remote Data copy = 0
- Local CPU Copy = 0
- Remote CPU Copy = 0

Example

This is an example of output from the **show platform hardware fed switch** {*switch_num* | **active** | **standby** } **forward summary** command.

```
Device#show platform hardware fed switch 1 forward summary
```

```
Time: Fri Sep 16 08:25:00 PDT 2016
```

```
Incomming Packet Details:
```

```
###[ Ethernet ]###
```

```
dst      = 00:51:0f:f2:0e:11
src      = 00:1d:01:85:ba:22
type     = ARP
```

```
###[ ARP ]###
```

```
hwtype   = 0x1
ptype    = IPv4
hwlen    = 6
plen     = 4
op       = is-at
hwsrc    = 00:1d:01:85:ba:22
psrc     = 10.10.1.33
hwdst    = 00:51:0f:f2:0e:11
pdst     = 10.10.1.1
```

```
Ingress:
```

```
Switch           : 1
Port              : GigabitEthernet1/0/1
Global Port Number : 1
Local Port Number : 1
Asic Port Number  : 21
ASIC Number       : 0
STP state         :
                  blkLrn31to0: 0xffdffffd
                  blkFwd31to0: 0xffdffffd
Vlan              : 1
Station Descriptor : 170
DestIndex         : 0xF009
DestModIndex      : 2
RewriteIndex      : 2
Forwarding Decision: FPS 2A L2 Destination
```

```
Replication Bitmap:
```

```
Local CPU copy   : 0
Local Data copy  : 1
Remote CPU copy  : 0
Remote Data copy : 0
```

```
Egress:
```

```
Switch           : 1
Outgoing Port     : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number       : 0
Vlan              : 1
```

show platform resources

To display platform resource information, use the **show platform resources** command in privileged EXEC mode.

show platform resources

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The output of this command displays the used memory, which is total memory minus the accurate free memory.

Example

The following is sample output from the **show platform resources** command:

```
Switch# show platform resources
```

```
**State Acronym: H - Healthy, W - Warning, C - Critical
```

Resource State	Usage	Max	Warning	Critical
Control Processor H	7.20%	100%	90%	95%
DRAM H	2701MB (69%)	3883MB	90%	95%

show platform software ilpower

To display the inline power details of all the PoE ports on the device, use the **show platform software ilpower** command in privileged EXEC mode.

```
show platform software ilpower {details | port {GigabitEthernet interface-number } | system slot-number }
```

Syntax Description	details	Displays inline power details for all the interfaces.
	port	Displays inline power port configuration.
	GigabitEthernet <i>interface-number</i>	The GigabitEthernet interface number. Values range from 0 to 9.
	system <i>slot-number</i>	Displays inline power system configuration.
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was modified. The keyword details argument was added.
	Cisco IOS XE Denali 16.1.1	The command was introduced.

Examples

The following is sample output from the **show platform software ilpower details** command:

```
Device# show platform software ilpower details
ILP Port Configuration for interface Gi1/0/1
  Initialization Done:    Yes
  ILP Supported:         Yes
  ILP Enabled:           Yes
  POST:                  Yes
  Detect On:              No
  Powered Device Detected:      No
  Powered Device Class Done:    No
  Cisco Powered Device:        No
  Power is On:                 No
  Power Denied:                No
  Powered Device Type:         Null
  Powerd Device Class:         Null
  Power State:                 NULL
  Current State:               NGWC_ILP_DETECTING_S
  Previous State:              NGWC_ILP_SHUT_OFF_S
  Requested Power in milli watts: 0
  Short Circuit Detected:      0
  Short Circuit Count:         0
  Cisco Powerd Device Detect Count: 0
  Spare Pair mode:            0
  IEEE Detect:                 Stopped
  IEEE Short:                  Stopped
  Link Down:                   Stopped
  Voltage sense:               Stopped
  Spare Pair Architecture:     1
```

show platform software ilpower

```
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On: 0
Powered Device power state: 0
Timer:
  Power Good: Stopped
  Power Denied: Stopped
  Cisco Powered Device Detect: Stopped
```

show platform software process list

To display the list of running processes on a platform, use the **show platform software process list** command in privileged EXEC mode.

```
show platform software process list switch {switch-number | active | standby} {0 | F0 | R0}
[{name process-name | process-id process-ID | sort memory | summary}]
```

Syntax Description	
switch <i>switch-number</i>	Displays information about the switch. Valid values for <i>switch-number</i> argument are from 0 to 9.
active	Displays information about the active instance of the switch.
standby	Displays information about the standby instance of the switch.
0	Displays information about the shared port adapters (SPA) Interface Processor slot 0.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
R0	Displays information about the Route Processor (RP) slot 0.
name process-name	(Optional) Displays information about the specified process.
process-id process-ID	(Optional) Displays information about the specified process ID.
sort	(Optional) Displays information sorted according to processes.
memory	(Optional) Displays information sorted according to memory.
summary	(Optional) Displays a summary of the process memory of the host device.

Command Modes Privileged EXE (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	The command was introduced.

Usage Guidelines Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show platform software process list switch active R0** command:

```
Switch# show platform software process list switch active R0 summary

Total number of processes: 278
  Running                  : 2
```

show platform software process list

```

Sleeping           : 276
Disk sleeping     : 0
Zombies           : 0
Stopped           : 0
Paging            : 0

Up time           : 8318
Idle time         : 0
User time         : 216809
Kernel time      : 78931

Virtual memory    : 12933324800
Pages resident   : 634061
Major page faults: 2228
Minor page faults: 3491744

Architecture     : mips64
Memory (kB)
  Physical       : 3976852
  Total          : 3976852
  Used           : 2766952
  Free           : 1209900
  Active         : 2141344
  Inactive       : 1589672
  Inact-dirty    : 0
  Inact-clean    : 0
  Dirty          : 4
  AnonPages     : 1306800
  Bounce         : 0
  Cached         : 1984688
  Commit Limit  : 1988424
  Committed As  : 3358528
  High Total    : 0
  High Free     : 0
  Low Total     : 3976852
  Low Free      : 1209900
  Mapped        : 520528
  NFS Unstable  : 0
  Page Tables   : 17328
  Slab          : 0
  VMmalloc Chunk: 1069542588
  VMmalloc Total: 1069547512
  VMmalloc Used : 2588
  Writeback     : 0
  HugePages Total: 0
  HugePages Free: 0
  HugePages Rsvd: 0
  HugePage Size : 2048

Swap (kB)
  Total         : 0
  Used          : 0
  Free          : 0
  Cached       : 0

Buffers (kB)     : 439528

Load Average
  1-Min         : 1.13
  5-Min         : 1.18
  15-Min        : 0.92

```

show platform software process slot switch

To display platform software process switch information, use the **show platform software process slot switch** command in privileged EXEC mode.

```
show platform software process slot switch {switch-number | active | standby} {0 | F0 | R0}
monitor [{cycles no-of-times [{interval delay [{lines number}]}}]
```

Syntax Description		
	<i>switch-number</i>	Switch number.
	active	Specifies the active instance.
	standby	Specifies the standby instance.
	0	Specifies the shared port adapter (SPA) interface processor slot 0.
	F0	Specifies the Embedded Service Processor (ESP) slot 0.
	R0	Specifies the Route Processor (RP) slot 0.
	monitor	Monitors the running processes.
	cycles <i>no-of-times</i>	(Optional) Sets the number of times to run monitor command. Valid values are from 1 to 4294967295. The default is 5.
	interval <i>delay</i>	(Optional) Sets a delay after each . Valid values are from 0 to 300. The default is 3.
	lines <i>number</i>	(Optional) Sets the number of lines of output displayed. Valid values are from 0 to 512. The default is 0.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

Examples The following is sample output from the **show platform software process slot switch active R0 monitor** command:

show platform software process slot switch

```
Switch# show platform software process slot switch active R0 monitor
```

```
top - 00:01:52 up 1 day, 11:20, 0 users, load average: 0.50, 0.68, 0.83
Tasks: 311 total, 2 running, 309 sleeping, 0 stopped, 0 zombie
Cpu(s): 7.4%us, 3.3%sy, 0.0%ni, 89.2%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 3976844k total, 3955036k used, 21808k free, 419312k buffers
Swap: 0k total, 0k used, 0k free, 1946764k cached
```

```

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  5693 root        20   0  3448 1368  912  R   7   0.0   0:00.07 top
 17546 root        20   0 2044m 244m  79m  S   7   6.3 186:49.08 fed main event
 18662 root        20   0 1806m 678m 263m  S   5  17.5 215:32.38 linux_iods-imag
 30276 root        20   0  171m  42m  33m  S   5   1.1 125:06.77 repm
 17835 root        20   0  935m  74m  63m  S   4   1.9  82:28.31 sif_mgr
 18534 root        20   0  182m 150m  10m  S   2   3.9   8:12.08 smand
     1 root        20   0  8440 4740 2184  S   0   0.1   0:09.52 systemd
     2 root        20   0     0     0     0  S   0   0.0   0:00.00 kthreadd
     3 root        20   0     0     0     0  S   0   0.0   0:02.86 ksoftirqd/0
     5 root         0  -20     0     0     0  S   0   0.0   0:00.00 kworker/0:0H
     7 root        RT   0     0     0     0  S   0   0.0   0:01.44 migration/0
     8 root        20   0     0     0     0  S   0   0.0   0:00.00 rcu_bh
     9 root        20   0     0     0     0  S   0   0.0   0:23.08 rcu_sched
    10 root        20   0     0     0     0  S   0   0.0   0:58.04 rcuc/0
    11 root        20   0     0     0     0  S   0   0.0 21:35.60 rcuc/1
    12 root        RT   0     0     0     0  S   0   0.0   0:01.33 migration/1

```

Related Commands

Command	Description
show processes cpu platform monitor location	Displays information about the CPU utilization of the IOS-XE processes.

show platform software status control-processor

To display platform software control-processor status, use the **show platform software status control-processor** command in privileged EXEC mode.

show platform software status control-processor [{brief}]

Syntax Description	brief (Optional) Displays a summary of the platform control-processor status.
---------------------------	--

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines	<p>Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.</p>
-------------------------	---

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show platform memory software status control-processor** command:

```
Switch# show platform software status control-processor

2-RP0: online, statistics updated 7 seconds ago
Load Average: healthy
  1-Min: 1.00, status: healthy, under 5.00
  5-Min: 1.21, status: healthy, under 5.00
 15-Min: 0.90, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3976852
  Used: 2766284 (70%), status: healthy
  Free: 1210568 (30%)
  Committed: 3358008 (84%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User: 4.40, System: 1.70, Nice: 0.00, Idle: 93.80
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
  User: 3.80, System: 1.20, Nice: 0.00, Idle: 94.90
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
  User: 7.00, System: 1.10, Nice: 0.00, Idle: 91.89
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 4.49, System: 0.69, Nice: 0.00, Idle: 94.80
  IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

3-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
  1-Min: 0.24, status: healthy, under 5.00
  5-Min: 0.27, status: healthy, under 5.00
```

show platform software status control-processor

```

15-Min: 0.32, status: healthy, under 5.00
Memory (kb): healthy
Total: 3976852
Used: 2706768 (68%), status: healthy
Free: 1270084 (32%)
Committed: 3299332 (83%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 4.50, System: 1.20, Nice: 0.00, Idle: 94.20
IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 5.20, System: 0.50, Nice: 0.00, Idle: 94.29
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 3.60, System: 0.70, Nice: 0.00, Idle: 95.69
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 3.00, System: 0.60, Nice: 0.00, Idle: 96.39
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

4-RP0: unknown, statistics updated 2 seconds ago
Load Average: healthy
1-Min: 0.21, status: healthy, under 5.00
5-Min: 0.24, status: healthy, under 5.00
15-Min: 0.24, status: healthy, under 5.00
Memory (kb): healthy
Total: 3976852
Used: 1452404 (37%), status: healthy
Free: 2524448 (63%)
Committed: 1675120 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 2.30, System: 0.40, Nice: 0.00, Idle: 97.30
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 4.19, System: 0.69, Nice: 0.00, Idle: 95.10
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 4.79, System: 0.79, Nice: 0.00, Idle: 94.40
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 2.10, System: 0.40, Nice: 0.00, Idle: 97.50
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

9-RP0: unknown, statistics updated 4 seconds ago
Load Average: healthy
1-Min: 0.20, status: healthy, under 5.00
5-Min: 0.35, status: healthy, under 5.00
15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
Total: 3976852
Used: 1451328 (36%), status: healthy
Free: 2525524 (64%)
Committed: 1675932 (42%), under 95%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.90, System: 0.50, Nice: 0.00, Idle: 97.60
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 4.39, System: 0.19, Nice: 0.00, Idle: 95.40
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 5.70, System: 1.00, Nice: 0.00, Idle: 93.30
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00

```

```

CPU3: CPU Utilization (percentage of time spent)
  User: 1.30, System: 0.60, Nice: 0.00, Idle: 98.00
  IRQ: 0.00, SIRQ: 0.10, IOWait: 0.00

```

The following is sample output from the **show platform memory software status control-processor brief** command:

```
Switch# show platform software status control-processor brief
```

```

Load Average
  Slot Status 1-Min 5-Min 15-Min
2-RP0 Healthy 1.10 1.21 0.91
3-RP0 Healthy 0.23 0.27 0.31
4-RP0 Healthy 0.11 0.21 0.22
9-RP0 Healthy 0.10 0.30 0.34

Memory (kB)
  Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
2-RP0 Healthy 3976852 2766956 (70%) 1209896 (30%) 3358352 (84%)
3-RP0 Healthy 3976852 2706824 (68%) 1270028 (32%) 3299276 (83%)
4-RP0 Healthy 3976852 1451888 (37%) 2524964 (63%) 1675076 (42%)
9-RP0 Healthy 3976852 1451580 (37%) 2525272 (63%) 1675952 (42%)

CPU Utilization
  Slot CPU User System Nice Idle IRQ SIRQ IOWait
2-RP0 0 4.10 2.00 0.00 93.80 0.00 0.10 0.00
      1 4.60 1.00 0.00 94.30 0.00 0.10 0.00
      2 6.50 1.10 0.00 92.40 0.00 0.00 0.00
      3 5.59 1.19 0.00 93.20 0.00 0.00 0.00
3-RP0 0 2.80 1.20 0.00 95.90 0.00 0.10 0.00
      1 4.49 1.29 0.00 94.20 0.00 0.00 0.00
      2 5.30 1.60 0.00 93.10 0.00 0.00 0.00
      3 5.80 1.20 0.00 93.00 0.00 0.00 0.00
4-RP0 0 1.30 0.80 0.00 97.89 0.00 0.00 0.00
      1 1.30 0.20 0.00 98.50 0.00 0.00 0.00
      2 5.60 0.80 0.00 93.59 0.00 0.00 0.00
      3 5.09 0.19 0.00 94.70 0.00 0.00 0.00
9-RP0 0 3.99 0.69 0.00 95.30 0.00 0.00 0.00
      1 2.60 0.70 0.00 96.70 0.00 0.00 0.00
      2 4.49 0.89 0.00 94.60 0.00 0.00 0.00
      3 2.60 0.20 0.00 97.20 0.00 0.00 0.00

```

show processes cpu platform monitor

To displays information about the CPU utilization of the IOS-XE processes, use the **show processes cpu platform monitor** command in privileged EXEC mode.

show processes cpu platform monitor location switch {*switch-number* | **active** | **standby**} {**0** | **F0** | **R0**}

Syntax Description	location	Displays information about the Field Replaceable Unit (FRU) location.
	switch	Specifies the switch.
	<i>switch-number</i>	Switch number.
	active	Specifies the active instance.
	standby	Specifies the standby instance.
	0	Specifies the shared port adapter (SPA) interface processor slot 0.
	F0	Specifies the Embedded Service Processor (ESP) slot 0.
	R0	Specifies the Route Processor (RP) slot 0.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines The output of the **show platform software process slot switch** and **show processes cpu platform monitor location** commands display the output of the Linux **top** command. The output of these commands display Free memory and Used memory as displayed by the Linux **top** command. The values displayed for the Free memory and Used memory by these commands do not match the values displayed by the output of other platform-memory related CLIs.

Examples

The following is sample output from the **show processes cpu monitor location switch active R0** command:

```
Switch# show processes cpu platform monitor location switch active R0

top - 00:04:21 up 1 day, 11:22,  0 users,  load average: 0.42, 0.60, 0.78
Tasks: 312 total,  4 running, 308 sleeping,  0 stopped,  0 zombie
Cpu(s):  7.4%us,  3.3%sy,  0.0%ni, 89.2%id,  0.0%wa,  0.0%hi,  0.1%si,  0.0%st
Mem:   3976844k total,  3956928k used,    19916k free,  419312k buffers
Swap:          0k total,          0k used,          0k free, 1947036k cached

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  6294 root        20   0  3448 1368  912  R   9.0   0.0   0:00.07 top
 17546 root        20   0 2044m 244m  79m  S   6.3 187:02.07 fed main event
30276 root        20   0  171m  42m  33m  S   7.1   1.1 125:15.54 repm
   16 root        20   0    0    0    0  S   5.0   0.0  22:07.92 rcuc/2
   21 root        20   0    0    0    0  R   5.0   0.0  22:13.24 rcuc/3
```

```

18662 root      20    0 1806m 678m 263m R    5 17.5 215:47.59 linux_iods-imag
  11 root      20    0     0   0   0 S    4  0.0  21:37.41 rcuc/1
10333 root      20    0 6420 3916 1492 S    4  0.1   4:47.03 btrace_rotate.s
  10 root      20    0     0   0   0 S    2  0.0   0:58.13 rcuc/0
 6304 root      20    0   776   12   0 R    2  0.0   0:00.01 ls
17835 root      20    0 935m  74m  63m S    2  1.9 82:34.07 sif_mgr
   1 root      20    0 8440 4740 2184 S    0  0.1   0:09.52 systemd
   2 root      20    0     0   0   0 S    0  0.0   0:00.00 kthreadd
   3 root      20    0     0   0   0 S    0  0.0   0:02.86 ksoftirqd/0
   5 root        0 -20     0   0   0 S    0  0.0   0:00.00 kworker/0:0H
   7 root      RT    0     0   0   0 S    0  0.0   0:01.44 migration/0

```

Related Commands

Command	Description
show platform software process slot switch	Displays platform software process switch information.

show processes memory platform

To display memory usage per Cisco IOS XE process, use the **show processes memory platform** command in privileged EXEC mode.

```
show processes memory platform [{detailed {name process-name | process-id process-ID} [{location | maps [{location}] | smaps [{location}]}] | location | sorted [{location}]}] switch {switch-number | active | standby} {0 | F0 | R0}
```

Syntax Description		
detailed <i>process-name</i>	(Optional) Displays detailed memory information for a specified Cisco IOS XE process.	
name <i>process-name</i>	(Optional) Matches the Cisco IOS XE process name.	
process-id <i>process-ID</i>	(Optional) Matches the Cisco IOS XE process ID.	
location	(Optional) Displays information about the FRU location.	
maps	(Optional) Displays memory maps of a process.	
smaps	(Optional) Displays smaps of a process.	
sorted	(Optional) Displays the sorted output based on the total memory used by Cisco IOS XE processes.	
switch <i>switch-number</i>	Displays information about the device.	
active	Displays information about the active instance of the switch.	
standby	Displays information about the standby instance of the switch.	
0	Displays information about the SPA-Inter-Processor slot 0.	
F0	Displays information about the Embedded Service Processor (ESP) slot 0.	
R0	Displays information about the Route Processor (RP) slot 0.	

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	The command was introduced.

Usage Guidelines

Prior to Cisco IOS XE Denali 16.3.1, the Free Memory displayed in the command output was obtained from the underlying Linux kernel. This value was not accurate because some memory chunks that was available for use was not considered as free memory.

In Cisco IOS XE Denali 16.3.1, the free memory is accurately computed and displayed in the Free Memory field of the command output.

Examples

The following is sample output from the **show processes memory platform** command:

```
Switch# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K
  Pid  Text      Data  Stack  Dynamic  RSS    Total      Name
-----
    1  1246     4400   132    1308    4400   8328      systemd
   96   233     2796   132     132    2796   12436     systemd-journal
  105   284     1796   132     176    1796   5208      systemd-udev
  707    52     2660   132     172    2660  11688     in.telnetd
  744   968     3264   132    1700    3264   5800      brelay.sh
  835    52     2660   132     172    2660  11688     in.telnetd
  863   968     3264   132    1700    3264   5800      brelay.sh
  928   968     3996   132    2312    3996   6412      reflector.sh
  933   968     3976   132    2312    3976   6412      droputil.sh
  934   968     2140   132     528    2140   4628      oom.sh
  936   173     936    132     132     936   3068      xinetd
  945   968     1472   132     132    1472   4168      libvirtd.sh
  947   592    43164   132    3096   43164  154716     repm
  954    45     932    132     132     932   3132      rpcbind
  986   482     3476   132     132    3476  169288     libvirtd
  988    66     940    132     132     940   2724      rpc.statd
  993   968     928    132     132     928   4232      boothelper_evt.
 1017   21     640    132     132     640   2500      inotifywait
 1089  102     1200   132     132    1200   3328      rpc.mountd
 1328    9     2940   132     148    2940  13844      rotee
 1353   39     532    132     132     532   2336      sleep
!
!
!
```

The following is sample output from the **show processes memory platform information** command:

```
Switch# show processes memory platform location switch active R0

System memory: 3976852K total, 2762844K used, 1214008K free,
Lowest: 1214008K
  Pid  Text      Data  Stack  Dynamic  RSS    Total      Name
-----
    1  1246     4400   132    1308    4400   8328      systemd
   96   233     2796   132     132    2796   12436     systemd-journal
  105   284     1796   132     176    1796   5208      systemd-udev
  707    52     2660   132     172    2660  11688     in.telnetd
  744   968     3264   132    1700    3264   5800      brelay.sh
  835    52     2660   132     172    2660  11688     in.telnetd
  863   968     3264   132    1700    3264   5800      brelay.sh
  928   968     3996   132    2312    3996   6412      reflector.sh
  933   968     3976   132    2312    3976   6412      droputil.sh
!
!
!
```

The following is sample output from the **show processes memory platform sorted** command:

```
Switch# show processes memory platform sorted

System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K
  Pid  Text      Data  Stack  Dynamic    RSS    Total      Name
-----
 9655  3787    264964  136   18004    264964  2675968      wcm
17261   324    248588  132   103908   248588  2093076    fed main event
 7885 149848   684864  136     80     684864  1853548   linux_iosd-imag
17891   398    75772  136   1888     75772   958240     sif_mgr
17067  1087    77912  136   1796    77912   702184     platform_mgr
 4268   391   102084  136   5596   102084   482656     cli_agent
 4856   357    93388  132   3680    93388   340052      dbm
29842  8722    64428  132   8056    64428   297068     fman_fp_image
 5960  9509    76088  136   3200    76088   287156     fman_rp
!
!
!
```

The following is sample output from the **show processes memory platform sorted location switch active R0** command:

```
Switch# show processes memory platform sorted location switch active R0

System memory: 3976852K total, 2763584K used, 1213268K free,
Lowest: 1213268K
  Pid  Text      Data  Stack  Dynamic    RSS    Total      Name
-----
 9655  3787    264968  136   18004    264968  2675968      wcm
17261   324    249020  132   103908   249020  2093076    fed main event
 7885 149848   684912  136     80     684912  1853548   linux_iosd-imag
17891   398    75884  136   1888     75884   958240     sif_mgr
17067  1087    77820  136   1796    77820   702184     platform_mgr
 4268   391   102084  136   5596   102084   482656     cli_agent
 4856   357    93388  132   3680    93388   340052      dbm
29842  8722    64428  132   8056    64428   297068     fman_fp_image
 5960  9509    76088  136   3200    76088   287156     fman_rp
!
!
!
```


show power inline

To display the Power over Ethernet (PoE) status for the specified PoE port, the specified stack member, or for all PoE ports in the switch stack, use the **show power inline** command in EXEC mode.

show power inline [{**police** | **priority**}] [{*interface-id* | **module** *stack-member-number*}] [**detail**]

Syntax Description	
police	(Optional) Displays the power policing information about real-time power consumption.
priority	(Optional) Displays the power inline port priority for each port.
<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.

```
Device> show power inline
Module   Available   Used   Remaining
         (Watts)    (Watts) (Watts)
-----
1         n/a         n/a    n/a
2         n/a         n/a    n/a
3         1440.0     15.4   1424.6
4         720.0      6.3    713.7
Interface Admin Oper   Power Device   Class Max
         (Watts)
-----
Gi3/0/1  auto  off   0.0   n/a     n/a  30.0
Gi3/0/2  auto  off   0.0   n/a     n/a  30.0
Gi3/0/3  auto  off   0.0   n/a     n/a  30.0
Gi3/0/4  auto  off   0.0   n/a     n/a  30.0
Gi3/0/5  auto  off   0.0   n/a     n/a  30.0
Gi3/0/6  auto  off   0.0   n/a     n/a  30.0
Gi3/0/7  auto  off   0.0   n/a     n/a  30.0
Gi3/0/8  auto  off   0.0   n/a     n/a  30.0
```

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:

```

Device> show power inline gigabitethernet1/0/1
Interface Admin Oper      Power  Device      Class Max
              (Watts)
-----
Gi1/0/1   auto   off      0.0   n/a         n/a   30.0

```

This is an example of output from the **show power inline module switch-number** command on stack member 3. The table that follows describes the output fields.

```

Device> show power inline module 3
Module   Available   Used   Remaining
         (Watts)    (Watts) (Watts)
-----
3        865.0      864.0   1.0
Interface Admin Oper      Power  Device      Class Max
              (Watts)
-----
Gi3/0/1   auto   power-deny  4.0   n/a         n/a   15.4
Gi3/0/2   auto   off         0.0   n/a         n/a   15.4
Gi3/0/3   auto   off         0.0   n/a         n/a   15.4
Gi3/0/4   auto   off         0.0   n/a         n/a   15.4
Gi3/0/5   auto   off         0.0   n/a         n/a   15.4
Gi3/0/6   auto   off         0.0   n/a         n/a   15.4
Gi3/0/7   auto   off         0.0   n/a         n/a   15.4
Gi3/0/8   auto   off         0.0   n/a         n/a   15.4
Gi3/0/9   auto   off         0.0   n/a         n/a   15.4
Gi3/0/10  auto   off         0.0   n/a         n/a   15.4
<output truncated>

```

Table 8: show power inline Field Descriptions

Field	Description
Available	The total amount of configured power ¹ 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.

¹ The configured power is the power that you manually specify or that the switch specifies by using CDP power negotiation or the IEEE classification, which is different than the real-time power that is monitored with the power sensing feature.

This is an example of output from the **show power inline police** command on a stacking-capable switch:

```
Device> show power inline police
Module   Available   Used   Remaining
         (Watts)    (Watts) (Watts)
-----
1         370.0      0.0    370.0
3         865.0      864.0   1.0

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.

```

Device> show power inline police gigabitethernet1/0/1
Interface Admin Oper Admin Oper Cutoff Oper
          State State Police Police Power Power
-----
Gi1/0/1 auto off none n/a n/a 0.0

```

Table 9: show power inline police Field Descriptions

Field	Description
Available	The total amount of configured power ² 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.

² 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.

```
Device> 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
```

show stack-power

To display information about StackPower stacks or switches in a power stack, use the **show stack-power** command in EXEC mode.

```
{show stack-power [{budgeting | detail | load-shedding | neighbors}] [order power-stack-name] |
[stack-name [stack-id] | switch [switch-id]]}
```

Syntax Description	
budgeting	(Optional) Displays the stack power budget table.
detail	(Optional) Displays the stack power stack details.
load-shedding	(Optional) Displays the stack power load shedding table.
neighbors	(Optional) Displays the stack power neighbor table.
order <i>power-stack-name</i>	(Optional) Displays the load shedding priority for a power stack. Note This keyword is available only after the load-shedding keyword.
stack-name	(Optional) Displays budget table, details, or neighbors for all power stacks or the specified power stack. Note This keyword is not available after the load-shedding keyword.
<i>stack-id</i>	(Optional) Power stack ID for the power stack. The stack ID must be 31 characters or less.
switch	(Optional) Displays budget table, details, load-shedding, or neighbors for all switches or the specified switch.
<i>switch-id</i>	(Optional) Switch ID for the switch. The switch number is from 1 to 9.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	Support for all the options was enabled for this command.
	Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines This command is available only on switch stacks running the IP Base or IP Services image.

If a switch is shut down because of load shedding, the output of the **show stack-power** command still includes the MAC address of the shutdown neighbor switch. The command output shows the stack power topology even if there is not enough power to power a switch.

Examples

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

show stack-power

```

Device# show stack-power
Power Stack      Stack  Stack  Total  Rsvd  Alloc  Unused  Num  Num
Name             Mode   Topolgy Pwr (W) Pwr (W) Pwr (W) Pwr (W) SW  PS
-----
Powerstack-1     SP-PS  Stndaln 350    150   200    0       1   1

```

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

```

Device# show stack-power budgeting
Power Stack      Stack  Stack  Total  Rsvd  Alloc  Unused  Num  Num
Name             Mode   Topolgy Pwr (W) Pwr (W) Pwr (W) Pwr (W) SW  PS
-----
Powerstack-1     SP-PS  Stndaln 350    150   200    0       1   1

      Power Stack      PS-A  PS-B  Power  Alloc  Avail  Consumd Pwr
SW  Name              (W)   (W)   Budgt (W) Power (W) Pwr (W) Sys/PoE (W)
--  -----
1   Powerstack-1     350   0     200    200    0      60 /0
-----
Totals:                200    0      60 /0

```


show 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:

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

show tech-support

To automatically run **show** commands that display system information, use the **show tech-support** command in the privilege EXEC mode.

show tech-support [{**cef** | **cft** | **eigrp** | **evc** | **fnf** | **ipc** | **ipmulticast** | **ipsec** | **mfib** | **nat** | **nbar** | **onep** | **ospf** | **page** | **password** | **rsvp** | **subscriber** | **vrrp** | **wccp**}]

Syntax Description

cef	(Optional) Displays CEF related information.
cft	(Optional) Displays CFT related information.
eigrp	(Optional) Displays EIGRP related information.
evc	(Optional) Displays EVC related information.
fnf	(Optional) Displays flexible netflow related information.
ipc	(Optional) Displays IPC related information.
ipmulticast	(Optional) Displays IP multicast related information.
ipsec	(Optional) Displays IPSEC related information.
mfib	(Optional) Displays MFIB related information.
nat	(Optional) Displays NAT related information.
nbar	(Optional) Displays NBAR related information.
onep	(Optional) Displays ONEP related information.
ospf	(Optional) Displays OSPF related information.
page	(Optional) Displays the command output on a single page at a time. Use the Return key to display the next line of output or use the space bar to display the next page of information. If not used, the output scrolls (that is, it does not stop for page breaks). Press the Ctrl-C keys to stop the command output.
password	(Optional) Leaves passwords and other security information in the output. If not used, passwords and other security-sensitive information in the output are replaced with the label "<removed>".
rsvp	(Optional) Displays IP RSVP related information.
subscriber	(Optional) Displays subscriber related information.
vrrp	(Optional) Displays VRRP related information.
wccp	(Optional) Displays WCCP related information.

Command Modes

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was enhanced to display of the outputs of the following commands in the output modifier : <ul style="list-style-type: none">• show power inline• show platform software ilpower details• show power inline police• show stack-power budgeting
	Cisco IOS XE Denali 16.1.1	This command was reintroduced.

Usage Guidelines

The output from the **show tech-support** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support > filename**) in the local writable storage file system or the remote file system. Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

You can use one of the following redirection methods:

- **> filename** - Redirects the output to a file.
- **>> filename** - Redirects the output to a file in append mode.

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:

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

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

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

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

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

stack-power

To configure StackPower parameters for the power stack or for a switch in the power stack, use the **stack power** command in global configuration mode. To return to the default setting, use the **no** form of the command,

```
stack-power {stack power-stack-name | switch stack-member-number}
no stack-power {stack power-stack-name | switch stack-member-number}
```

Syntax Description	stack <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:

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

switchport block

To prevent unknown multicast or unicast packets from being forwarded, use the **switchport block** command in interface configuration mode. To allow forwarding unknown multicast or unicast packets, use the **no** form of this command.

```
switchport block {multicast | unicast}
no switchport block {multicast | unicast}
```

Syntax Description	<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>Device(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>				

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:

```
Device(config)# system mtu 6000
Global Ethernet MTU is set to 6000 bytes.
Note: this is the Ethernet payload size, not the total
Ethernet frame size, which includes the Ethernet
header/trailer and possibly other tags, such as ISL or
802.1q tags.
```

test mcu read-register

To enable debugging of the Power over Ethernet (PoE) controller, use the **test mcu read-register** command in privileged EXEC mode.

test mcu read-register {**det-cls-offset** | **manufacture-id** | **port-mode**}

Syntax Description	
det-cls-offset	Displays the read detection classification register summary.
manufacture-id	Displays the PoE controller manufacture ID.
port-mode	Displays the port mode details.

Command Modes Privileged EXEC

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

Examples

The following is sample output from the **test mcu read-register det-cls-offset** command:

```
Device# test mcu read-register det-cls-offset 1
DETECTION ENABLE BIT SUMMARY
```

Controller	port1	port2	port3	port4	register (hexadecimal)
1	1	0	1	0	5
2	1	0	1	0	5
3	1	0	1	0	5
4	1	0	1	0	5
5	1	0	1	0	5
6	1	0	1	0	5
7	1	0	1	0	5
8	1	0	1	0	5
9	1	0	1	0	5
10	1	0	1	0	5
11	0	0	1	0	4
12	1	0	0	0	1

```
CLASSIFICATION ENABLE BIT SUMMARY
```

Controller	port1	port2	port3	port4	register (hexadecimal)
1	1	0	1	0	5
2	1	0	1	0	5
3	1	0	1	0	5
4	1	0	1	0	5
5	1	0	1	0	5
6	1	0	1	0	5
7	1	0	1	0	5
8	1	0	1	0	5
9	1	0	1	0	5
10	1	0	1	0	5
11	0	0	1	0	4
12	1	0	0	0	1

1	1	0	1	0	5
2	1	0	1	0	5
3	1	0	1	0	5
4	1	0	1	0	5
5	1	0	1	0	5
6	1	0	1	0	5
7	1	0	1	0	5
8	1	0	1	0	5
9	1	0	1	0	5
10	1	0	1	0	5
11	0	0	1	0	4
12	1	0	0	0	1

The following is sample output from the **test mcu read-register manufacture-id** command:

```
MANUFACTURE ID : DEVICE_BCM_PALPATINE reg_val = 0x1B
```

The following is sample output from the **test mcu read-register port-mode** command:

```
PORT MODE SUMMERY
```

Controller	port1	port2	port3	port4	register (hexadecimal)
1	01	00	01	00	22
2	01	00	01	00	22
3	01	00	01	00	22
4	01	00	01	00	22
5	01	00	01	00	22
6	01	00	01	00	22
7	01	00	01	00	22
8	01	00	01	00	22
9	01	00	01	00	22
10	01	00	01	00	22
11	00	00	01	00	20
12	01	00	00	00	2

voice-signaling vlan (network-policy configuration)

To create a network-policy profile for the voice-signaling application type, use the **voice-signaling vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice-signaling vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos cos-value	(Optional) Specifies the Layer 2 priority class of service (CoS) for the configured VLAN. The range is 0 to 7; the default is 5.
dscp dscp-value	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice-signaling application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

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

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice-signaling application type is for network topologies that require a different policy for voice signaling than for voice media. This application type should not be advertised if all of the same network policies apply as those advertised in the voice policy TLV.

When you are in network-policy profile configuration mode, you can create the profile for voice-signaling by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure voice-signaling for VLAN 200 with a priority 2 CoS:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice-signaling vlan 200 cos 2
```

This example shows how to configure voice-signaling for VLAN 400 with a DSCP value of 45:

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

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

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

voice vlan (network-policy configuration)

To create a network-policy profile for the voice application type, use the **voice vlan** command in network-policy configuration mode. To delete the policy, use the **no** form of this command.

```
voice vlan {vlan-id [{cos cos-value | dscp dscp-value}] | dot1p [{cos l2-priority | dscp dscp}] | none | untagged}
```

Syntax Description

vlan-id	(Optional) The VLAN for voice traffic. The range is 1 to 4094.
cos <i>cos-value</i>	(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 <i>dscp-value</i>	(Optional) Specifies the differentiated services code point (DSCP) value for the configured VLAN. The range is 0 to 63; the default is 46.
dot1p	(Optional) Configures the phone to use IEEE 802.1p priority tagging and to use VLAN 0 (the native VLAN).
none	(Optional) Does not instruct the Cisco IP phone about the voice VLAN. The phone uses the configuration from the phone key pad.
untagged	(Optional) Configures the phone to send untagged voice traffic. This is the default for the phone.

Command Default

No network-policy profiles for the voice application type are defined.

The default CoS value is 5.

The default DSCP value is 46.

The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

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

Usage Guidelines

Use the **network-policy profile** global configuration command to create a profile and to enter network-policy profile configuration mode.

The voice application type is for dedicated IP telephones and similar devices that support interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security through isolation from data applications.

When you are in network-policy profile configuration mode, you can create the profile for voice by specifying the values for VLAN, class of service (CoS), differentiated services code point (DSCP), and tagging mode.

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).

To return to privileged EXEC mode from the network-policy profile configuration mode, enter the **exit** command.

This example shows how to configure the voice application type for VLAN 100 with a priority 4 CoS:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 cos 4
```

This example shows how to configure the voice application type for VLAN 100 with a DSCP value of 34:

```
Device(config)# network-policy profile 1
Device(config-network-policy)# voice vlan 100 dscp 34
```

This example shows how to configure the voice application type for the native VLAN with priority tagging:

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




PART **III**

IP

- [IP](#), on page 139



IP

- [clear ip nhrp](#), on page 141
- [debug nhrp](#), on page 142
- [fhrp delay](#), on page 144
- [fhrp version vrrp v3](#), on page 145
- [glbp authentication](#), on page 146
- [glbp forwarder preempt](#), on page 148
- [glbp ip](#), on page 149
- [glbp load-balancing](#), on page 151
- [glbp name](#), on page 152
- [glbp preempt](#), on page 154
- [glbp priority](#), on page 155
- [glbp timers](#), on page 156
- [glbp weighting](#), on page 158
- [glbp weighting track](#), on page 159
- [ip address dhcp](#), on page 161
- [ip address pool \(DHCP\)](#), on page 164
- [ip address](#), on page 165
- [ip http server](#), on page 168
- [ip http secure-server](#), on page 170
- [ip nhrp map](#), on page 172
- [ip nhrp map multicast](#), on page 174
- [ip nhrp network-id](#), on page 176
- [ip nhrp nhs](#), on page 177
- [ipv6 nd cache expire](#), on page 179
- [ipv6 nd na glean](#), on page 180
- [ipv6 nd nud retry](#), on page 181
- [key chain](#), on page 183
- [key-string \(authentication\)](#), on page 184
- [key](#), on page 185
- [show glbp](#), on page 187
- [show ip nhrp nhs](#), on page 190
- [show ip ports all](#), on page 192
- [show key chain](#), on page 194

- [show track](#), on page 195
- [track](#), on page 197
- [vrrp](#), on page 199
- [vrrp description](#), on page 200
- [vrrp preempt](#), on page 201
- [vrrp priority](#), on page 202
- [vrrp timers advertise](#), on page 203
- [vrrs leader](#), on page 205

clear ip nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the **clear ip nhrp** command in user EXEC or privileged EXEC mode.

```
clear ip nhrp [{vrf {vrf-name | global}}] [{dest-ip-address [{dest-mask}] | tunnel number | counters
[interface tunnel number]}] stats [{tunnel number [{vrf {vrf-name | global}}]}]
```

Syntax Description	Parameter	Description
	vrf	(Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.
	<i>vrf-name</i>	(Optional) Name of the VRF address family to which the command is applied.
	global	(Optional) Specifies the global VRF instance.
	<i>dest-ip-address</i>	(Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.
	<i>dest-mask</i>	(Optional) Destination network mask.
	counters	(Optional) Clears the NHRP counters.
	interface	(Optional) Clears the NHRP mapping entries for all interfaces.
	tunnel number	(Optional) Removes the specified interface from the NHRP cache.
	stats	(Optional) Clears all IPv4 statistic information for all interfaces.

Command Modes	Mode
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The **clear ip nhrp** command does not clear any static (configured) IP-to-NBMA address mappings from the NHRP cache.

Examples The following example shows how to clear all dynamic entries from the NHRP cache for an interface:

```
Switch# clear ip nhrp
```

Related Commands	Command	Description
	show ip nhrp	Displays NHRP mapping information.

debug nhrp

To enable Next Hop Resolution Protocol (NHRP) debugging, use the **debug nhrp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug nhrp [{**attribute** | **cache** | **condition** {**interface** **tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address* *nbma-name* *ipv6-nbma-address*} } } | **unmatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate**}]

no debug nhrp [{**attribute** | **cache** | **condition** {**interface** **tunnel** *number* | **peer** {**nbma** {*ipv4-nbma-address* *nbma-name* *ipv6-nbma-address*} } } | **unmatched** | **vrf** *vrf-name*} | **detail** | **error** | **extension** | **group** | **packet** | **rate**}]

Syntax Description

attribute	(Optional) Enables NHRP attribute debugging operations.
cache	(Optional) Enables NHRP cache debugging operations.
condition	(Optional) Enables NHRP conditional debugging operations.
interface tunnel <i>number</i>	(Optional) Enables debugging operations for the tunnel interface.
nbma	(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.
<i>ipv4-nbma-address</i>	(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.
<i>nbma-name</i>	(Optional) NBMA network name.
<i>IPv6-address</i>	(Optional) Enables debugging operations based on the IPv6 address of the NBMA network. Note The <i>IPv6-address</i> argument is not supported in Cisco IOS XE Denali 16.3.1.
vrf <i>vrf-name</i>	(Optional) Enables debugging operations for the virtual routing and forwarding instance.
detail	(Optional) Displays detailed logs of NHRP debugs.
error	(Optional) Enables NHRP error debugging operations.
extension	(Optional) Enables NHRP extension processing debugging operations.
group	(Optional) Enables NHRP group debugging operations.
packet	(Optional) Enables NHRP activity debugging.
rate	(Optional) Enables NHRP rate limiting.
routing	(Optional) Enables NHRP routing debugging operations.

Command Default

NHRP debugging is not enabled.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines



Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *IPv6-nbma-address* argument although available on the switch, will not work if configured.

Use the **debug nhrp detail** command to view the NHRP attribute logs.

The **Virtual-Access number** keyword-argument pair is visible only if the virtual access interface is available on the device.

Examples

The following sample output from the **debug nhrp** command displays NHRP debugging output for IPv4:

```
Switch# debug nhrp

Aug  9 13:13:41.486: NHRP: Attempting to send packet via DEST 10.1.1.99
Aug  9 13:13:41.486: NHRP: Encapsulation succeeded. Tunnel IP addr 10.11.11.99
Aug  9 13:13:41.486: NHRP: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug  9 13:13:41.486:      src: 10.1.1.11, dst: 10.1.1.99
Aug  9 13:13:41.486: NHRP: 105 bytes out Tunnel0
Aug  9 13:13:41.486: NHRP: Receive Registration Reply via Tunnel0 vrf 0, packet size: 125
Aug  9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

Related Commands

Command	Description
show ip nhrp	Displays NHRP mapping information.

fhrp delay

To specify the delay period for the initialization of First Hop Redundancy Protocol (FHRP) clients, use the **fhrp delay** command in interface configuration mode. To remove the delay period specified, use the **no** form of this command.

```
fhrp delay { [minimum] [reload] seconds }
no fhrp delay { [minimum] [reload] seconds }
```

Syntax Description	
minimum	(Optional) Configures the delay period after an interface becomes available.
reload	(Optional) Configures the delay period after the device reloads.
<i>seconds</i>	Delay period in seconds. The range is from 0 to 3600.

Command Default None

Command Modes Interface configuration (config-if)

Examples This example shows how to specify the delay period for the initialization of FHRP clients:

```
Device(config-if)# fhrp delay minimum 90
```

Related Commands	Command	Description
	show fhrp	Displays First Hop Redundancy Protocol (FHRP) information.

fhrp version vrrp v3

To enable Virtual Router Redundancy Protocol version 3 (VRRPv3) and Virtual Router Redundancy Service (VRRS) configuration on a device, use the **fhrp version vrrp v3** command in global configuration mode. To disable the ability to configure VRRPv3 and VRRS on a device, use the **no** form of this command.

fhrp version vrrp v3
no fhrp version vrrp v3

Syntax Description	This command has no keywords or arguments.
Command Default	VRRPv3 and VRRS configuration on a device is not enabled.
Command Modes	Global configuration (config)
Usage Guidelines	When VRRPv3 is in use, VRRP version 2 (VRRPv2) is unavailable.

Examples

In the following example, a tracking process is configured to track the state of an IPv6 object using a VRRPv3 group. VRRP on GigabitEthernet interface 0/0/0 then registers with the tracking process to be informed of any changes to the IPv6 object on the VRRPv3 group. If the IPv6 object state on serial interface VRRPv3 goes down, then the priority of the VRRP group is reduced by 20:

```
Device(config)# fhrp version vrrp v3
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# vrrp 1 address-family ipv6
Device(config-if-vrrp)# track 1 decrement 20
```

Related Commands

Command	Description
track (VRRP)	Enables an object to be tracked using a VRRPv3 group.

glbp authentication

To configure an authentication string for the Gateway Load Balancing Protocol (GLBP), use the **glbp authentication** command in interface configuration mode. To disable authentication, use the **no** form of this command.

```
glbp group-numberauthentication {text string | md5 {key-string [{0 | 7}] key | key-chain name-of-chain}}
```

```
no glbp group-number authentication {text string | md5 {key-string [{0 | 7}] key | key-chain name-of-chain}}
```

Syntax Description

<i>group-number</i>	GLBP group number in the range from 0 to 1023.
text <i>string</i>	Specifies an authentication string. The number of characters in the command plus the text string must not exceed 255 characters.
md5	Message Digest 5 (MD5) authentication.
key-string <i>key</i>	Specifies the secret key for MD5 authentication. The key string cannot exceed 100 characters in length. We recommend using at least 16 characters.
0	(Optional) Unencrypted key. If no prefix is specified, the key is unencrypted.
7	(Optional) Encrypted key.
key-chain <i>name-of-chain</i>	Identifies a group of authentication keys.

Command Default

No authentication of GLBP messages occurs.

Command Modes

Interface configuration (config-if)

Usage Guidelines

The same authentication method must be configured on all the devices that are configured to be members of the same GLBP group, to ensure interoperability. A device will ignore all GLBP messages that contain the wrong authentication information.

If password encryption is configured with the **service password-encryption** command, the software saves the key string in the configuration as encrypted text.

Examples

The following example configures stringxyz as the authentication string required to allow GLBP devices in group 10 to interoperate:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 authentication text stringxyz
```

In the following example, GLBP queries the key chain “AuthenticateGLBP” to obtain the current live key and key ID for the specified key chain:

```
Device(config)# key chain AuthenticateGLBP
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string ThisIsASecretKey
Device(config-keychain-key)# exit
```

```
Device(config-keychain)# exit
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# glbp 2 authentication md5 key-chain AuthenticateGLBP
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp forwarder preempt

To configure a device to take over as active virtual forwarder (AVF) for a Gateway Load Balancing Protocol (GLBP) group if the current AVF falls below its low weighting threshold, use the **glbp forwarder preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

glbp group forwarder preempt [*delay minimum seconds*]
no glbp group forwarder preempt [*delay minimum*]

Syntax Description		
	<i>group</i>	GLBP group number in the range from 0 to 1023.
	delay minimum <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the device will delay before taking over the role of AVF. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default Forwarder preemption is enabled with a default delay of 30 seconds.

Command Modes Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Examples

The following example shows a device being configured to preempt the current AVF when the current AVF falls below its low weighting threshold. If the device preempts the current AVF, it waits 60 seconds before taking over the role of the AVF.

```
Device(config-if)# glbp 10 forwarder preempt delay minimum 60
```

Related Commands

Command	Description
glbp ip	Enables GLBP.

glbp ip

To activate the Gateway Load Balancing Protocol (GLBP), use the **glbp ip** command in interface configuration mode. To disable GLBP, use the **no** form of this command.

```
glbp group ip [ip-address [secondary]]
no glbp group ip [ip-address [secondary]]
```

Syntax Description		
	<i>group</i>	GLBP group number in the range from 0 to 1023.
	<i>ip-address</i>	(Optional) Virtual IP address for the GLBP group. The IP address must be in the same subnet as the interface IP address.
	secondary	(Optional) Indicates that the IP address is a secondary GLBP virtual address.

Command Default GLBP is disabled by default.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines The **glbp ip** command activates GLBP on the configured interface. If an IP address is specified, that address is used as the designated virtual IP address for the GLBP group. If no IP address is specified, the designated address is learned from another device configured to be in the same GLBP group. For GLBP to elect an active virtual gateway (AVG), at least one device on the cable must have been configured with the designated address. A device must be configured with, or have learned, the virtual IP address of the GLBP group before assuming the role of a GLBP gateway or forwarder. Configuring the designated address on the AVG always overrides a designated address that is in use.

When the **glbp ip** command is enabled on an interface, the handling of proxy Address Resolution Protocol (ARP) requests is changed (unless proxy ARP was disabled). ARP requests are sent by hosts to map an IP address to a MAC address. The GLBP gateway intercepts the ARP requests and replies to the ARP on behalf of the connected nodes. If a forwarder in the GLBP group is active, proxy ARP requests are answered using the MAC address of the first active forwarder in the group. If no forwarder is active, proxy ARP responses are suppressed.

Examples

The following example activates GLBP for group 10 on GigabitEthernet interface 1/0/1. The virtual IP address to be used by the GLBP group is set to 10.21.8.10.

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 ip 10.21.8.10
```

Related Commands

Command	Description
show glbp	Displays GLBP information.

glbp load-balancing

To specify the load-balancing method used by the active virtual gateway (AVG) of the Gateway Load Balancing Protocol (GLBP), use the **glbp load-balancing** command in interface configuration mode. To disable load balancing, use the **no** form of this command.

```
glbp group load-balancing [{host-dependent | round-robin | weighted}]
no glbp group load-balancing
```

Syntax Description	group	GLBP group number in the range from 0 to 1023.
	host-dependent	(Optional) Specifies a load balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged.
	round-robin	(Optional) Specifies a load balancing method where each virtual forwarder in turn is included in address resolution replies for the virtual IP address. This method is the default.
	weighted	(Optional) Specifies a load balancing method that is dependent on the weighting value advertised by the gateway.

Command Default The round-robin method is the default.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines Use the host-dependent method of GLBP load balancing when you need each host to always use the same device. Use the weighted method of GLBP load balancing when you need unequal load balancing because devices in the GLBP group have different forwarding capacities.

Examples The following example shows the host-dependent load-balancing method being configured for the AVG of the GLBP group 10:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip 10.21.8.10
Device(config-if)# glbp 10 load-balancing host-dependent
```

Related Commands	Command	Description
	show glbp	Displays GLBP information.

glbp name

To enable IP redundancy by assigning a name to the Gateway Load Balancing Protocol (GLBP) group, use the **glbp name** command in interface configuration mode. To disable IP redundancy for a group, use the **no** form of this command.

glbp *group-number* **name** *group-name*
no glbp *group-number* **name** *group-name*

Syntax Description	
<i>group-number</i>	GLBP group number. Range is from 0 to 1023.
<i>group-name</i>	GLBP group name specified as a character string. Maximum number of characters is 255.

Command Default IP redundancy for a group is disabled.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines The GLBP redundancy client must be configured with the same GLBP group name so that the redundancy client and the GLBP group can be connected.

Examples The following example assigns the abccomp name to GLBP group 10:

```
Device(config-if)# glbp 10 name abccomp
```

Related Commands	Command	Description
	glbp authentication	Configures an authentication string for the GLBP.
	glbp forwarder preempt	Configures a device to take over as AVF for a GLBP group if it has higher priority than the current AVF.
	glbp ip	Activates GLBP.
	glbp load-balancing	Specifies the load-balancing method used by the AVG of GLBP.
	glbp preempt	Configures the gateway to take over as AVG for a GLBP group if it has higher priority than the current AVG.
	glbp priority	Sets the priority level of the gateway within a GLBP group.
	glbp timers	Configures the time between hello packets sent by the GLBP gateway and the time for which the virtual gateway and virtual forwarder information is considered valid.

Command	Description
glbp timers redirect	Configures the time during which the AVG for a GLBP group continues to redirect clients to a secondary AVF.
glbp weighting	Specifies the initial weighting value of the GLBP gateway.
glbp weighting track	Specifies a tracking object where the GLBP weighting changes based on the availability of the object being tracked.
show glbp	Displays GLBP information.
track	Configures an interface to be tracked where the GLBP weighting changes based on the state of the interface.

glbp preempt

To configure the gateway to take over as active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group if it has higher priority than the current AVG, use the **glbp preempt** command in interface configuration mode. To disable this function, use the **no** form of this command.

```
glbp group preempt [delay minimum seconds]
no glbp group preempt [delay minimum]
```

Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
delay minimum <i>seconds</i>	(Optional) Specifies a minimum number of seconds that the device will delay before taking over the role of AVG. The range is from 0 to 3600 seconds with a default delay of 30 seconds.

Command Default

A GLBP device with a higher priority than the current AVG cannot assume the role of AVG. The default delay value is 30 seconds.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Examples

The following example shows a device being configured to preempt the current AVG when its priority of 254 is higher than that of the current AVG. If the device preempts the current AVG, it waits 60 seconds before assuming the role of AVG.

```
Device(config-if)# glbp 10 preempt delay minimum 60
Device(config-if)# glbp 10 priority 254
```

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp priority	Sets the priority level of the device within a GLBP group.

glbp priority

To set the priority level of the gateway within a Gateway Load Balancing Protocol (GLBP) group, use the **glbp priority** command in interface configuration mode. To remove the priority level of the gateway, use the **no** form of this command.

glbp group priority level
no glbp group priority level

Syntax Description	
<i>group</i>	GLBP group number in the range from 0 to 1023.
<i>level</i>	Priority of the gateway within the GLBP group. The range is from 1 to 255. The default is 100.

Command Default The GLBP virtual gateway preemptive scheme is disabled

Command Modes Interface configuration (config-if)

Usage Guidelines Use this command to control which virtual gateway becomes the active virtual gateway (AVG). After the priorities of several different virtual gateways are compared, the gateway with the numerically higher priority is elected as the AVG. If two virtual gateways have equal priority, the gateway with the higher IP address is selected.

Examples

The following example shows a virtual gateway being configured with a priority of 254:

```
Device(config-if)# glbp 10 priority 254
```

Related Commands	Command	Description
	glbp ip	Enables GLBP.
	glbp preempt	Configures a device to take over as the AVG for a GLBP group if it has higher priority than the current AVG.

glbp timers

To configure the time between hello packets sent by the Gateway Load Balancing Protocol (GLBP) gateway and the time that the virtual gateway and virtual forwarder information is considered valid, use the **glbp timers** command in interface configuration mode. To restore the timers to their default values, use the **no** form of this command.

```
glbp group timers {hellotime{holdtime | msec holdtime} | msec { holdtime | msec holdtime}
| redirect time-interval-to-redirect | timeout}
no glbp group timers {hellotime{holdtime | msec holdtime} | msec { holdtime | msec
holdtime} | redirect time-interval-to-redirect | timeout}
```

Syntax Description

<i>group</i>	GLBP group number in the range from 0 to 1023.
msec	(Optional) Specifies that the following (<i>hellotime</i> or <i>holdtime</i>) argument value will be expressed in milliseconds rather than seconds.
<i>hellotime</i>	Hello interval. The default is 3 seconds (3000 milliseconds).
<i>holdtime</i>	Time before the virtual gateway and virtual forwarder information contained in the hello packet is considered invalid. The default is 10 seconds (10,000 milliseconds).
redirect	Specifies time interval during which the active virtual gateway (AVG) for a Gateway Load Balancing Protocol (GLBP) group continues to redirect clients to a secondary active virtual forwarder (AVF) and time-out values for failed forwarders.
<i>time-interval-to-redirect</i>	The redirect timer interval in the range from 0 to 3600 seconds. The default is 600 seconds (10 minutes). Note The zero value for the <i>time-interval-to-redirect</i> argument cannot be removed from the range of acceptable values because preexisting configurations of Cisco IOS software already using the zero value could be negatively affected during an upgrade. However, be advised that a zero setting is not recommended and <i>time-interval-to-redirect</i> , if used, results in a redirect timer that never expires. If the redirect timer does not expire, then when a device fails, new hosts continue to be assigned to the failed device instead of being redirected to the backup.
<i>timeout</i>	The time interval, in the range from 600 to 64,800 seconds, before the secondary virtual forwarder becomes unavailable. The default is 14,400 seconds (4 hours).

Command Default

GLBP timers are set to their default values.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

Devices on which timer values are not configured can learn timer values from the active virtual gateway (AVG). The timers configured on the AVG always override any other timer settings. All devices in a GLBP group should use the same timer values. If a GLBP gateway sends a hello message, the information should be considered valid for one holdtime. Normally, holdtime is greater than three times the value of hello time, ($holdtime > 3 * hellotime$). The range of values for holdtime force the holdtime to be greater than the hello time.

Examples

The following example shows the GLBP group 10 on GigabitEthernet interface 1/0/1 timers being configured for an interval of 5 seconds between hello packets, and the time after which virtual gateway and virtual forwarder information is considered to be invalid to 18 seconds:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# glbp 10 ip
Device(config-if)# glbp 10 timers 5 18
```

Related Commands

Command	Description
glbp ip	Activates GLBP.
show glbp	Displays GLBP information.

glbp weighting

To specify the initial weighting value of the Gateway Load Balancing Protocol (GLBP) gateway, use the **glbp weighting** command in interface configuration mode. To restore the default values, use the **no** form of this command.

```
glbp group weighting maximum [lower lower] [upper upper]
no glbp group weighting
```

Syntax Description		
<i>group</i>		GLBP group number in the range from 0 to 1023.
<i>maximum</i>		Maximum weighting value in the range from 1 to 254. Default value is 100.
lower <i>lower</i>		(Optional) Specifies a lower weighting value in the range from 1 to the specified maximum weighting value. Default value is 1.
upper <i>upper</i>		(Optional) Specifies an upper weighting value in the range from the lower weighting to the maximum weighting value. The default value is the specified maximum weighting value.

Command Default The default gateway weighting value is 100 and the default lower weighting value is 1.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines The weighting value of a virtual gateway is a measure of the forwarding capacity of the gateway. If a tracked interface on the device fails, the weighting value of the device may fall from the maximum value to below the lower threshold, causing the device to give up its role as a virtual forwarder. When the weighting value of the device rises above the upper threshold, the device can resume its active virtual forwarder role.

Use the **glbp weighting track** and **track** commands to configure parameters for an interface to be tracked. If an interface on a device goes down, the weighting for the device can be reduced by a specified value.

Examples The following example shows the weighting of the gateway for GLBP group 10 being set to a maximum of 110 with a lower weighting limit of 95 and an upper weighting limit of 105:

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

Related Commands	Command	Description
	glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.
	track	Configures an interface to be tracked.

glbp weighting track

To specify a tracking object where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the availability of the object being tracked, use the **glbp weighting track** command in interface configuration mode. To remove the tracking, use the **no** form of this command.

```
glbp group weighting track object-number [decrement value]
no glbp group weighting track object-number [decrement value]
```

Syntax Description		
	<i>group</i>	GLBP group number in the range from 0 to 1023.
	<i>object-number</i>	Object number representing an item to be tracked. The valid range is 1 to 1000. Use the track command to configure the tracked object.
	decrement value	(Optional) Specifies an amount by which the GLBP weighting for the device is decremented (or incremented) when the interface goes down (or comes back up). The value range is from 1 to 254, with a default value of 10.

Command Default Objects are not tracked for GLBP weighting changes.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines This command ties the weighting of the GLBP gateway to the availability of its interfaces. It is useful for tracking interfaces that are not configured for GLBP.

When a tracked interface goes down, the GLBP gateway weighting decreases by 10. If an interface is not tracked, its state changes do not affect the GLBP gateway weighting. For each GLBP group, you can configure a separate list of interfaces to be tracked.

The optional *value* argument specifies by how much to decrement the GLBP gateway weighting when a tracked interface goes down. When the tracked interface comes back up, the weighting is incremented by the same amount.

When multiple tracked interfaces are down, the configured weighting decrements are cumulative.

Use the **track** command to configure each interface to be tracked.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, GigabitEthernet interface 1/0/1 tracks two interfaces represented by the numbers 1 and 2. If interface 1 goes down, the GLBP gateway weighting decreases by the default value of 10. If interface 2 goes down, the GLBP gateway weighting decreases by 5.

```
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting track 1
Device(config-if)# glbp 10 weighting track 2 decrement 5
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
track	Configures an interface to be tracked.

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp** command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

```
ip address dhcp [client-id interface-type number] [hostname hostname]
no ip address dhcp [client-id interface-type number] [hostname hostname]
```

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The client-id <i>interface-type number</i> option sets the client identifier to the hexadecimal MAC address of the named interface.
<i>interface-type</i>	(Optional) Interface type. For more information, use the question mark (?) online help function.
<i>number</i>	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
<i>hostname</i>	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the device. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The client-id keyword and <i>interface-type number</i> argument were added.
12.2(3)	This command was modified. The hostname keyword and <i>hostname</i> argument were added. The behavior of the client-id <i>interface-type number</i> option changed. See the “Usage Guidelines” section for details.
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelines



Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the device.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id interface-type number hostname hostname** command is when *interface-type* is the Ethernet interface where the command is configured and *interface-type number* is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id interface-type number** option overrides the default and forces the use of the hexadecimal MAC address of the named interface.



Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco device is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the device. However, you can use the **ip address dhcp hostname hostname** command to place a different name in the DHCP option 12 field than the globally configured hostname of the device.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 10: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains “cisco- <i>mac-address</i> -Eth1” in the client ID field. The <i>mac-address</i> is the MAC address of the Ethernet 1 interface and contains the default hostname of the device in the option 12 field.

Configuration Method	Contents of DISCOVER Messages
ip address dhcp hostname <i>hostname</i>	The DISCOVER message contains “cisco- <i>mac-address</i> -Eth1” in the client ID field. The <i>mac-address</i> is the MAC address of the Ethernet 1 interface, and contains <i>hostname</i> in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the device in the option 12 field.
ip address dhcp client-id ethernet 1 hostname <i>hostname</i>	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains <i>hostname</i> in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a device configured as shown in the following example would contain “cisco- *mac-address* -Eth1” in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp
```

The DISCOVER message sent by a device configured as shown in the following example would contain “cisco- *mac-address* -Eth1” in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface GigabitEthernet 1/0/1
 ip address dhcp hostname def
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1
```

The DISCOVER message sent by a device configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id GigabitEthernet 1/0/1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address pool (DHCP)

To enable the IP address of an interface to be automatically configured when a Dynamic Host Configuration Protocol (DHCP) pool is populated with a subnet from IP Control Protocol (IPCP) negotiation, use the **ip address pool** command in interface configuration mode. To disable autoconfiguring of the IP address of the interface, use the **no** form of this command.

ip address pool *name*

no ip address pool

Syntax Description

<i>name</i>	Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in <i>name</i> .
-------------	---

Command Default

IP address pooling is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use this command to automatically configure the IP address of a LAN interface when there are DHCP clients on the attached LAN that should be serviced by the DHCP pool on the device. The DHCP pool obtains its subnet dynamically through IPCP subnet negotiation.

Examples

The following example specifies that the IP address of GigabitEthernet interface 1/0/1 will be automatically configured from the address pool named abc:

```
ip dhcp pool abc
  import all
  origin ipcp
!
interface GigabitEthernet 1/0/1
  ip address pool abc
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.

ip address

To set a primary or secondary IP address for an interface, use the **ip address** command in interface configuration mode. To remove an IP address or disable IP processing, use the no form of this command.

```
ip address ip-address mask [secondary [vrf vrf-name]]
no ip address ip-address mask [secondary [vrf vrf-name]]
```

Syntax Description

<i>ip-address</i>	IP address.
<i>mask</i>	Mask for the associated IP subnet.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. Note If the secondary address is used for a VRF table configuration with the vrf keyword, the vrf keyword must be specified also.
vrf	(Optional) Name of the VRF table. The <i>vrf-name</i> argument specifies the VRF name of the ingress interface.

Command Default

No IP address is defined for the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines

An interface can have one primary IP address and multiple secondary IP addresses. Packets generated by the Cisco IOS software always use the primary IP address. Therefore, all devices and access servers on a segment should share the same primary network number.

Hosts can determine subnet masks using the Internet Control Message Protocol (ICMP) mask request message. Devices respond to this request with an ICMP mask reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the software detects another host using one of its IP addresses, it will print an error message on the console.

The optional **secondary** keyword allows you to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and Address Resolution Protocol (ARP) requests are handled properly, as are interface routes in the IP routing table.

Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There may not be enough host addresses for a particular network segment. For example, your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you need 300 host addresses. Using

secondary IP addresses on the devices or access servers allows you to have two logical subnets using one physical subnet.

- Many older networks were built using Level 2 bridges. The judicious use of secondary addresses can aid in the transition to a subnetted, device-based network. Devices on an older, bridged segment can be easily made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. This situation is not permitted when subnets are in use. In these instances, the first network is *extended*, or layered on top of the second network using secondary addresses.



Note If any device on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.



Note When you are routing using the Open Shortest Path First (OSPF) algorithm, ensure that all secondary addresses of an interface fall into the same OSPF area as the primary addresses.

To transparently bridge IP on an interface, you must perform the following two tasks:

- Disable IP routing (specify the **no ip routing** command).
- Add the interface to a bridge group, see the **bridge-group** command.

To concurrently route and transparently bridge IP on an interface, see the **bridge crb** command.

Examples

In the following example, 192.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for GigabitEthernet interface 1/0/1:

```
interface GigabitEthernet 1/0/1
 ip address 192.108.1.27 255.255.255.0
 ip address 192.31.7.17 255.255.255.0 secondary
```

Related Commands

Command	Description
match ip route-source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show ip interface	Displays the usability status of interfaces configured for IP.

Command	Description
show route-map	Displays static and dynamic route maps.

ip http server

To enable the HTTP server on your IP or IPv6 system, including the Cisco web browser user interface, enter the **ip http server** command in global configuration mode. To disable the HTTP server, use the **no** form of this command..

ip http server
no ip http server

Syntax Description This command has no arguments or keywords.

Command Default The HTTP server uses the standard port 80 by default.
 HTTP/TCP port 8090 is open by default.

Command Modes Global configuration (config)

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

Usage Guidelines The command enables both IPv4 and IPv6 access to the HTTP server. However, an access list configured with the **ip http access-class** command is applied only to IPv4 traffic. IPv6 traffic filtering is not supported.



Caution The standard HTTP server and the secure HTTP (HTTPS) server can run on a system at the same time. If you enable the HTTPS server using the **ip http secure-server** command, disable the standard HTTP server using the **no ip http server** command to ensure that secure data cannot be accessed through the standard HTTP connection.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

The following example shows how to enable the HTTP server on both IPv4 and IPv6 systems.

After enabling the HTTP server, you can set the base path by specifying the location of the HTML files to be served. HTML files used by the HTTP web server typically reside in system flash memory. Remote URLs can be specified using this command, but use of remote path names (for example, where HTML files are located on a remote TFTP server) is not recommended.

```
Device(config)#ip http server
Device(config)#ip http path flash:
```

Related Commands

Command	Description
ip http access-class	Specifies the access list that should be used to restrict access to the HTTP server.
ip http path	Specifies the base path used to locate files for use by the HTTP server.

Command	Description
ip http secure-server	Enables the HTTPS server.

ip http secure-server

To enable a secure HTTP (HTTPS) server, enter the **ip http secure-server** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command..

ip http secure-server
no ip http secure-server

Syntax Description This command has no arguments or keywords.

Command Default The HTTPS server is disabled.

Command Modes Global configuration (config)

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

Usage Guidelines The HTTPS server uses the Secure Sockets Layer (SSL) version 3.0 protocol.



Caution

When enabling an HTTPS server, you should always disable the standard HTTP server to prevent unsecured connections to the same services. Disable the standard HTTP server using the **no ip http server** command in global configuration mode (this step is precautionary; typically, the HTTP server is disabled by default).

If a certificate authority (CA) is used for certification, you should declare the CA trustpoint on the routing device before enabling the HTTPS server.

To close HTTP/TCP port 8090, you must disable both the HTTP and HTTPS servers. Enter the **no http server** and the **no http secure-server** commands, respectively.

Examples

In the following example the HTTPS server is enabled, and the (previously configured) CA trustpoint CA-trust-local is specified:

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#ip http secure-server
Device(config)#ip http secure-trustpoint CA-trust-local
Device(config)#end

Device#show ip http server secure status
HTTP secure server status: Enabled
HTTP secure server port: 443
HTTP secure server ciphersuite: 3des-ede-cbc-sha des-cbc-sha rc4-128-md5 rc4-12a
HTTP secure server client authentication: Disabled
HTTP secure server trustpoint: CA-trust-local
```

Related Commands

Command	Description
ip http secure-trustpoint	Specifies the CA trustpoint that should be used for obtaining signed certificates for the HTTPS server.
ip http server	Enables the HTTP server on an IP or IPv6 system, including the Cisco web browser user interface.
show ip http server secure status	Displays the configuration status of the HTTPS server.

ip nhrp map

To statically configure the IP-to-nonbroadcast multiaccess (NBMA) address mapping of IP destinations connected to an NBMA network, use the **ip nhrp map** command in interface configuration mode. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the **no** form of this command.

```
ip nhrp map ip-address [ip-nbma-address | destination-mask [{ip-nbma-address ipv6-nbma-address}]
ipv6-nbma-address]
no ip nhrp map ip-address [ip-nbma-address | destination-mask [{ip-nbma-address ipv6-nbma-address}]
ipv6-nbma-address]
```

Syntax Description

<i>ip-address</i>	IP address of the destinations reachable through the NBMA network. This address is mapped to the NBMA address.
<i>ip-nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium; for example, ATM has a Network Service Access Point (NSAP) address, Ethernet has a MAC address, and Switched Multimegabit Data Service (SMDS) has an E.164 address. This address is mapped to the IP address.
<i>destination-mask</i>	Destination address mask.
<i>ipv6-nbma-address</i>	IPv6 NBMA address. Note This argument is not supported in Cisco IOS XE Denali 16.3.1.

Command Default

No static IP-to-NBMA cache entries exist.

Command Modes

Interface configuration(config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

In Cisco IOS XE Denali 16.3.1, NHRP supports only hub-to-spoke communication; spoke-to-spoke communication is not supported.



Note

In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

Configure at least one static mapping to reach the next-hop server. To statistically configure multiple IP-to-NBMA address mappings, configure this command multiple times.

When using the routing protocols, Open Shortest Path First (OSPF) or Enhanced Interior Gateway Routing Protocol (EIGRP), configure the **ip ospf network point-to-multipoint** (when OSPF is used for hub-to-spoke communication) and **ip split-horizon eigrp** (when EIGRP is used) commands on the tunnel to allow the traffic.

Examples

In the following example, this station in a multipoint tunnel network is statically configured to be served by two next-hop servers 10.0.0.1 and 10.0.1.3. The NBMA address for 10.0.0.1 is statically configured as 192.0.2.1 and the NBMA address for 10.0.1.3 is 198.51.100.1.

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip nhrp nhs 10.0.0.1
Switch(config-if)# ip nhrp nhs 10.0.1.3
Switch(config-if)# ip nhrp map 10.0.0.1 192.0.2.1
Switch(config-if)# ip nhrp map 10.0.1.3 198.51.100.1
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
ip split-horizon eigrp	Enables EIGRP split horizon.
ip ospf network point-to-multipoint	Configures the OSPF network type to point-to-multipoint.

ip nhrp map multicast

To configure nonbroadcast multiaccess (NBMA) addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network, use the **ip nhrp map multicast** command in interface configuration mode. To remove the destinations, use the **no** form of this command.

```
ip nhrp map multicast {ip-nbma-address ipv6-nbma-address | dynamic}
no ip nhrp map multicast {ip-nbma-address ipv6-nbma-address | dynamic}
```

Syntax Description

<i>ip-nbma-address</i>	NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium that you are using.
<i>ipv6-nbma-address</i>	IPv6 NBMA address. Note This argument is not supported in Cisco IOS XE Denali 16.3.1.
dynamic	Dynamically learns destinations from client registrations on the hub.

Command Default

No NBMA addresses are configured as destinations for broadcast or multicast packets.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines



Note In Cisco IOS XE Denali 16.3.1, this command supports only IPv4; the *ipv6-nbma-address* argument although available on the switch, will not work if configured.

This command applies only to tunnel interfaces. This command is useful for supporting broadcasts over a tunnel network when the underlying network does not support IP multicast. If the underlying network does support IP multicast, you should use the **tunnel destination** command to configure a multicast destination for transmission of tunnel broadcasts or multicasts.

When multiple NBMA addresses are configured, the system replicates the broadcast packet for each address.

Examples

In the following example, if a packet is sent to 10.255.255.255, it is replicated to destinations 10.0.0.1 and 10.0.0.2:

```
Switch(config)# interface tunnel 0
Switch(config-if)# ip address 10.0.0.3 255.0.0.0
Switch(config-if)# ip nhrp map multicast 10.0.0.1
Switch(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

Command	Description
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.
tunnel destination	Specifies the destination for a tunnel interface.

ip nhrp network-id

To enable the Next Hop Resolution Protocol (NHRP) on an interface, use the **ip nhrp network-id** command in interface configuration mode. To disable NHRP on the interface, use the **no** form of this command.

ip nhrp network-id *number*
no ip nhrp network-id [{*number*}]

Syntax Description

<i>number</i>	Globally unique, 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network. The range is from 1 to 4294967295.
---------------	---

Command Default

NHRP is disabled on an interface.

Command Modes

Interface configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

In general, all NHRP stations within one logical NBMA network must be configured with the same network identifier.

Examples

The following example enables NHRP on the interface:

```
Switch(config-if)# ip nhrp network-id 1
```

Related Commands

Command	Description
clear ip nhrp	Clears all dynamic entries from the NHRP cache.
debug nhrp	Enables NHRP debugging.
interface	Configures an interface and enters interface configuration mode.

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs** command in interface configuration mode. To remove the address, use the **no** form of this command.

```
ip nhrp nhs {nhs-address [nbma {nbma-address FQDN-string}] [multicast] [priority value] [cluster value] | cluster value max-connections value | dynamic nbma {nbma-address FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
no ip nhrp nhs {nhs-address [nbma {nbma-address FQDN-string}] [multicast] [priority value] [cluster value] | cluster value max-connections value | dynamic nbma {nbma-address FQDN-string} [multicast] [priority value] [cluster value] | fallback seconds}
```

Syntax Description

<i>nhs-address</i>	Address of the next-hop server being specified.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
<i>nbma-address</i>	NBMA address.
<i>FQDN-string</i>	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies the use of NBMA mapping for broadcasts and multicasts.
priority value	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster value	(Optional) Specifies NHS groups. The range is from 0 to 10.
max-connections value	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback seconds	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Command Default

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating the **ip nhrp nhs** command with the same *nhs-address* argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Switch# configure terminal
Switch(config)# interface tunnel 1
Switch(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

ipv6 nd cache expire

To configure the duration of time before an IPv6 neighbor discovery cache entry expires, use the **ipv6 nd cache expire** command in the interface configuration mode. To remove this configuration, use the **no** form of this command.

```
ipv6 nd cache expire expire-time-in-seconds [refresh]
no ipv6 nd cache expire expire-time-in-seconds [refresh]
```

Syntax Description

Syntax Description	<i>expire-time-in-seconds</i>	The time range is from 1 through 65536 seconds. The default is 14400 seconds or 4 hours.
	refresh	(Optional) Automatically refreshes the neighbor discovery cache entry.

Command Modes

Interface configuration (config-if)

Command History

Command History

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

Usage Guidelines

By default, a neighbor discovery cache entry is expired and deleted if it remains in the STALE state for 14,400 seconds or 4 hours. The **ipv6 nd cache expire** command allows the expiry time to vary and to trigger auto refresh of an expired entry before the entry is deleted.

When the **refresh** keyword is used, a neighbor discovery cache entry is auto refreshed. The entry moves into the DELAY state and the neighbor unreachability detection process occurs, in which the entry transitions from the DELAY state to the PROBE state after 5 seconds. When the entry reaches the PROBE state, a neighbor solicitation is sent and then retransmitted as per the configuration.

Examples

The following example shows that the neighbor discovery cache entry is configured to expire in 7200 seconds or 2 hours:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd cache expire 7200
```

Related Commands

Command	Description
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd na glean

To configure the neighbor discovery to glean an entry from an unsolicited neighbor advertisement, use the **ipv6 nd na glean** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd na glean
no ipv6 nd na glean

Command Modes Interface configuration

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

Usage Guidelines IPv6 nodes may emit a multicast unsolicited neighbor advertisement packet following the successful completion of duplicate address detection (DAD). By default, other IPv6 nodes ignore these unsolicited neighbor advertisement packets. The **ipv6 nd na glean** command configures the router to create a neighbor advertisement entry on receipt of an unsolicited neighbor advertisement packet (assuming no such entry already exists and the neighbor advertisement has the link-layer address option). Use of this command allows a device to populate its neighbor advertisement cache with an entry for a neighbor before data traffic exchange with the neighbor.

Examples

The following example shows how to configure neighbor discovery to glean an entry from an unsolicited neighbor advertisement:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd na glean
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery cache entry expires.
ipv6 nd nud retry	Configures the number of times neighbor unreachability detection resends neighbor solicitations.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

ipv6 nd nud retry

To configure the number of times the neighbor unreachability detection process resends neighbor solicitations, use the **ipv6 nd nud retry** command in the interface configuration mode. To disable this feature, use the **no** form of this command.

```
ipv6 nd nud retry base interval max-attempts {final-wait-time}
no ipv6 nd nud retry base interval max-attempts {final-wait-time}
```

Syntax Description		
<i>base</i>	The neighbor unreachability detection process base value.	
<i>interval</i>	The time interval, in milliseconds, between retries. The range is from 1000 to 32000.	
<i>max-attempts</i>	The maximum number of retry attempts, depending on the base value. The range is from 1 to 128.	
<i>final-wait-time</i>	The waiting time, in milliseconds, on the last probe. The range is from 1000 to 32000.	

Command Modes Interface configuration (config-if)

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

Usage Guidelines When a device runs neighbor unreachability detection to resolve the neighbor detection entry for a neighbor again, it sends three neighbor solicitation packets 1 second apart. In certain situations, for example, spanning-tree events, or high-traffic events, or end-host reloads), three neighbor solicitation packets that are sent at an interval of 1 second may not be sufficient. To help maintain the neighbor cache in such situations, use the **ipv6 nd nud retry** command to configure exponential timers for neighbor solicitation retransmits.

The maximum number of retry attempts is configured using the *max-attempts* argument. The retransmit interval is calculated with the following formula:

$$tm^n$$

here,

- t = Time interval
- m = Base (1, 2, or 3)
- n = Current neighbor solicitation number (where the first neighbor solicitation is 0).

Therefore, **ipv6 nd nud retry 3 1000 5** command retransmits at intervals of 1,3,9,27,81 seconds. If the final wait time is not configured, the entry remains for 243 seconds before it is deleted.

The **ipv6 nd nud retry** command affects only the retransmit rate for the neighbor unreachability detection process, and not for the initial resolution, which uses the default of three neighbor solicitation packets sent 1 second apart.

Examples

The following example shows how to configure a fixed interval of 1 second and three retransmits:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 1 1000 3
```

The following example shows how to configure a retransmit interval of 1, 2, 4, and 8:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 2 1000 4
```

The following example shows how to configure the retransmit intervals of 1, 3, 9, 27, 81:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/4
Device(config-if)# ipv6 nd nud retry 3 1000 5
```

Related Commands

Command	Description
ipv6 nd cache expire	Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.
ipv6 nd na glean	Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.
show ipv6 interface	Displays the usability status of interfaces that are configured for IPv6.

key chain

To define an authentication key chain needed to enable authentication for routing protocols and enter key-chain configuration mode, use the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command.

key chain *name-of-chain*
no key chain *name-of-chain*

Syntax Description	<i>name-of-chain</i>	Name of a key chain. A key chain must have at least one key and can have up to 2147483647 keys.
---------------------------	----------------------	---

Command Default No key chain exists.

Command Modes Global configuration (config)

Usage Guidelines You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the **key chain** command, you enter key chain configuration mode.

Examples

The following example shows how to specify key chain:

```
Device(config-keychain-key)# key-string chestnut
```

Related Commands	Command	Description
	accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
	key	Identifies an authentication key on a key chain.
	key-string (authentication)	Specifies the authentication string for a key.
	send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
	show key chain	Displays authentication key information.

key-string (authentication)

To specify the authentication string for a key, use the **key-string**(authentication) command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

key-string *key-string* *text*

no *key-string* *text*

Syntax Description

<i>text</i>	Authentication string that must be sent and received in the packets using the routing protocol being authenticated. The string can contain from 1 to 80 uppercase and lowercase alphanumeric characters.
-------------	--

Command Default

No authentication string for a key exists.

Command Modes

Key chain key configuration (config-keychain-key)

Examples

The following example shows how to specify the authentication string for a key:

```
Device (config-keychain-key) # key-string key1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.
key	Identifies an authentication key on a key chain.
key chain	Defines an authentication key-chain needed to enable authentication for routing protocols.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

key

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

key *key-id*
no key *key-id*

Syntax Description

<i>key-id</i>	Identification number of an authentication key on a key chain. The range of keys is from 0 to 2147483647. The key identification numbers need not be consecutive.
---------------	---

Command Default

No key exists on the key chain.

Command Modes

Key-chain configuration (config-keychain)

Command History

Release	Modification
11.1	This command was introduced.
12.4(6)T	Support for IPv6 was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and Message Digest 5 (MD5) authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will continue and an error message will be generated. To disable authentication, you must manually delete the last valid key.

To remove all keys, remove the key chain by using the **no key chain** command.

Examples

The following example shows how to specify a key to identify authentication on a key-chain:

```
Device(config-keychain)# key 1
```

Related Commands

Command	Description
accept-lifetime	Sets the time period during which the authentication key on a key chain is received as valid.

Command	Description
key chain	Defines an authentication key chain needed to enable authentication for routing protocols.
key-string (authentication)	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.
show key chain	Displays authentication key information.

show glbp

To display Gateway Load Balancing Protocol (GLBP) information, use the **show glbp** command in privileged EXEC mode.

capability [*interface-type interface-number*]
interface-type interface-number [*group-number*] [*state*] [**brief**]

Syntax Description	capability	(Optional) Displays the GLBP capability interfaces.
	<i>interface-type interface-number</i>	(Optional) Interface type and number for which output is displayed.
	<i>group-number</i>	(Optional) GLBP group number in the range from 0 to 1023.
	<i>state</i>	(Optional) State of the GLBP device, one of the following: active , disabled , init , listen , and standby .
	brief	(Optional) Summarizes each virtual gateway or virtual forwarder with a single line of output.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced..

Usage Guidelines Use the **show glbp** command to display information about GLBP groups on a device. The **brief** keyword displays a single line of information about each virtual gateway or virtual forwarder. The **capability** keyword displays all GLBP-capable interfaces.

Examples

The following is sample output from the **show glbp** command that displays GLBP group 10:

```
Device# show glbp GigabitEthernet 1/0/1 10
GigabitEthernet1/0/1 - Group 10
  State is Active
    1 state change, last state change 00:04:52
  Virtual IP address is 10.21.8.10
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.608 secs
  Redirect time 600 sec, forwarder time-out 14400 sec
  Preemption disabled
  Active is local
  Standby is unknown
  Priority 100 (default)
  Weighting 100 (default 100), thresholds: lower 1, upper 100
  Load balancing: round-robin
  Group members:
    ac7e.8a35.6364 (10.21.8.32) local
  There is 1 forwarder (1 active)
  Forwarder 1
    State is Active
```

```

    1 state change, last state change 00:04:41
    MAC address is 0007.b400.0a01 (default)
    Owner ID is ac7e.8a35.6364
    Redirection enabled
    Preemption enabled, min delay 30 sec
    Active is local, weighting 100

```

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

Table 11: show glbp Field Descriptions

Field	Description
GigabitEthernet1/0/1 - Group	Interface type and number and GLBP group number for the interface.
State is	<p>State of the virtual gateway or virtual forwarder. For a virtual gateway, the state can be one of the following:</p> <ul style="list-style-type: none"> • Active--The gateway is the active virtual gateway (AVG) and is responsible for responding to Address Resolution Protocol (ARP) requests for the virtual IP address. • Disabled--The virtual IP address has not been configured or learned yet, but another GLBP configuration exists. • Initial--The virtual IP address has been configured or learned, but virtual gateway configuration is not complete. An interface must be up and configured to route IP, and an interface IP address must be configured. • Listen--The virtual gateway is receiving hello packets and is ready to change to the “speak” state if the active or standby virtual gateway becomes unavailable. • Speak--The virtual gateway is attempting to become the active or standby virtual gateway. • Standby--The gateway is next in line to be the AVG.
Virtual IP address is	The virtual IP address of the GLBP group. All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as “duplicate.” A duplicate address indicates that the device has failed to defend its ARP cache entry.
Hello time, hold time	The hello time is the time between hello packets (in seconds or milliseconds). The hold time is the time (in seconds or milliseconds) before other devices declare the active device to be down. All devices in a GLBP group use the hello- and hold-time values of the current AVG. If the locally configured values are different, the configured values appear in parentheses after the hello- and hold-time values.
Next hello sent in	The time until GLBP will send the next hello packet (in seconds or milliseconds).
Preemption	<p>Whether GLBP gateway preemption is enabled. If enabled, the minimum delay is the time (in seconds) for which a higher-priority nonactive device will wait before preempting the lower-priority active device.</p> <p>This field is also displayed under the forwarder section where it indicates GLBP forwarder preemption.</p>

Field	Description
Active is	The active state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the current AVG. This field is also displayed under the forwarder section where it indicates the address of the current AVF.
Standby is	The standby state of the virtual gateway. The value can be “local,” “unknown,” or an IP address. The address (and the expiration date of the address) is the address of the standby gateway (the gateway that is next in line to be the AVG).
Weighting	The initial weighting value with lower and upper threshold values.
Track object	The list of objects that are being tracked and their corresponding states.
IP redundancy name is	The name of the GLBP group.

Related Commands

Command	Description
glbp ip	Enables GLBP.
glbp timers	Configures the time between hello messages and the time before other devices declare the active GLBP device to be down.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs** command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [{*interface*}] [**detail**] [{**redundancy** [{*cluster number* | **preempted** | **running** | **waiting**}]}

Syntax Description

<i>interface</i>	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.
redundancy	(Optional) Displays information about NHS redundancy stacks.
<i>cluster number</i>	(Optional) Displays redundancy cluster information.
preempted	(Optional) Displays information about NHS that failed to become active and is preempted.
running	(Optional) Displays NHSs that are currently in Responding or Expecting replies states.
waiting	(Optional) Displays NHSs awaiting to be scheduled.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.



Note

The valid types can vary according to the platform and interfaces on the platform.

Table 12: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
ANI	0 to 1000	Autonomic-Networking virtual interface
Auto-Template	1 to 999	Auto-Template interface
GMPLS	0 to 1000	Multiprotocol Label Switching (MPLS) interface
GigabitEthernet	0 to 9	GigabitEthernet IEEE 802.3z
InternalInterface	0 to 9	Internal interface

Valid Types	Number Ranges	Interface Descriptions
LISP	0 to 65520	Locator/ID Separation Protocol (LISP) virtual interface
loopback	0 to 2147483647	Loopback interface
Null	0 to 0	Null interface
PROTECTION_GROUP	0 to 0	Protection-group controller
Port-channel	1 to 128	Port channel interface
TenGigabitEthernet	0 to 9	TenGigabitEthernet interface
Tunnel	0 to 2147483647	Tunnel interface
Tunnel-tp	0 to 65535	MPLS Transport Profile interface
Vlan	1 to 4094	VLAN interface

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Switch# show ip nhrp nhs detail

Legend:
  E=Expecting replies
  R=Responding
Tunnell:
  10.1.1.1          E req-sent 128 req-failed 1 repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64 NHS 10.1.1.1
```

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

Table 13: show ip nhrp nhs Field Descriptions

Field	Description
Tunnell	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.

show ip ports all

To display all the open ports on a device, use the **show ip ports all** in user EXEC or privileged EXEC mode.

show ip ports all

Syntax Description

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 Everest 16.5.1a	This command was introduced.

Usage Guidelines

This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

Examples

The following is sample output from the **show ip ports all** command:

```
Device#
show ip ports all
Proto Local Address Foreign Address State PID/Program Name
TCB Local Address Foreign Address (state)
tcp *:4786 *:* LISTEN 224/[IOS]SMI IBC server process
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:443 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
tcp *:80 *:* LISTEN 286/[IOS]HTTP CORE
udp *:10002 *:* 0/[IOS] Unknown
udp *:2228 10.0.0.0:0 318/[IOS]L2TRACE SERVER
```

The table below describes the significant fields shown in the display

Table 14: Field Descriptions of show ip ports all

Field	Description
Protocol	Transport protocol used.
Local Address.	Device IP Address.
Foreign Address	Remote or peer address.
State	State of the connection. It can be listen, established or connected.

Field	Description
PID/Program Name	Process ID or name

Related Commands

Command	Description
show tcp brief all	Displays information about TCP connection endpoints.
show ip sockets	Displays IP sockets information.

show key chain

To display the keychain, use the **show key chain** command.

show key chain [*name-of-chain*]

Syntax Description

<i>name-of-chain</i>	(Optional) Name of the key chain to display, as named in the key chain command.
----------------------	---

Command Default

If the command is used without any parameters, then it lists out all the key chains.

Command Modes

Privileged EXEC (#)

Examples

The following is sample output from the **show key chain** command:

```

show key chain
Device# show key chain

Key-chain AuthenticationGLBP:
  key 1 -- text "Thisisasecretkey"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]
Key-chain glbp2:
  key 100 -- text "abc123"
    accept lifetime (always valid) - (always valid) [valid now]
    send lifetime (always valid) - (always valid) [valid now]

```

Related Commands

Command	Description
key-string	Specifies the authentication string for a key.
send-lifetime	Sets the time period during which an authentication key on a key chain is valid to be sent.

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

```
show track [{object-number [brief] | application [brief] | interface [brief] | ip[route [brief] | [sla [brief]] | ipv6 [route [brief]] | list [route [brief]] | resolution [ip | ipv6] | stub-object [brief] | summary | timers}]
```

Syntax Description

<i>object-number</i>	(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
application	(Optional) Displays tracked application objects.
interface	(Optional) Displays tracked interface objects.
ip route	(Optional) Displays tracked IP route objects.
ip sla	(Optional) Displays tracked IP SLA objects.
ipv6 route	(Optional) Displays tracked IPv6 route objects.
list	(Optional) Displays the list of boolean objects.
resolution	(Optional) Displays resolution of tracked parameters.
summary	(Optional) Displays the summary of the specified object.
timers	(Optional) Displays polling interval timers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
XE 3.10S	This command was modified. The output was enhanced to display IPv6 route information.

Usage Guidelines

Use this command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

The following example shows information about the state of IP routing on the interface that is being tracked:

```
Device# show track 1

Track 1
  Interface GigabitEthernet 1/0/1 ip routing
  IP routing is Down (no IP addr)
  1 change, last change 00:01:08
```

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

Table 15: show track Field Descriptions

Field	Description
Track	Object number that is being tracked.
Interface GigabitEthernet 1/0/1 ip routing	Interface type, interface number, and object that is being tracked.
IP routing is	State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.
1 change, last change	Number of times that the state of a tracked object has changed and the time (in <i>hh:mm:ss</i>) since the last change.

Related Commands

Command	Description
show track resolution	Displays the resolution of tracked parameters.
track interface	Configures an interface to be tracked and enters tracking configuration mode.
track ip route	Tracks the state of an IP route and enters tracking configuration mode.

track

To configure an interface to be tracked where the Gateway Load Balancing Protocol (GLBP) weighting changes based on the state of the interface, use the **track** command in global configuration mode. To remove the tracking, use the **no** form of this command.

```
track object-number interface type number {line-protocol | ip routing | ipv6 routing}
no track object-number interface type number {line-protocol | ip routing | ipv6 routing}
```

Syntax Description		
	<i>object-number</i>	Object number in the range from 1 to 1000 representing the interface to be tracked.
	interface <i>type number</i>	Interface type and number to be tracked.
	line-protocol	Tracks whether the interface is up.
	ip routing	Tracks whether IP routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.
	ipv6 routing	Tracks whether IPv6 routing is enabled, an IP address is configured on the interface, and the interface state is up, before reporting to GLBP that the interface is up.

Command Default The state of the interfaces is not tracked.

Command Modes Global configuration (config)

Usage Guidelines Use the **track** command in conjunction with the **glbp weighting** and **glbp weighting track** commands to configure parameters for an interface to be tracked. If a tracked interface on a GLBP device goes down, the weighting for that device is reduced. If the weighting falls below a specified minimum, the device will lose its ability to act as an active GLBP virtual forwarder.

A maximum of 1000 objects can be tracked. Although 1000 tracked objects can be configured, each tracked object uses CPU resources. The amount of available CPU resources on a device is dependent upon variables such as traffic load and how other protocols are configured and run. The ability to use 1000 tracked objects is dependent upon the available CPU. Testing should be conducted on site to ensure that the service works under the specific site traffic conditions.

Examples

In the following example, TenGigabitEthernet interface 0/0/1 tracks whether GigabitEthernet interfaces 1/0/1 and 1/0/3 are up. If either of the GigabitEthernet interface goes down, the GLBP weighting is reduced by the default value of 10. If both GigabitEthernet interfaces go down, the GLBP weighting will fall below the lower threshold and the device will no longer be an active forwarder. To resume its role as an active forwarder, the device must have both tracked interfaces back up, and the weighting must rise above the upper threshold.

```
Device(config)# track 1 interface GigabitEthernet 1/0/1 line-protocol
Device(config-track)# exit
Device(config)# track 2 interface GigabitEthernet 1/0/3 line-protocol
Device(config-track)# exit
Device(config)# interface TenGigabitEthernet 0/0/1
Device(config-if)# ip address 10.21.8.32 255.255.255.0
Device(config-if)# glbp 10 weighting 110 lower 95 upper 105
```

```
Device(config-if)# glbp 10 weighting track 1  
Device(config-if)# glbp 10 weighting track 2
```

Related Commands

Command	Description
glbp weighting	Specifies the initial weighting value of a GLBP gateway.
glbp weighting track	Specifies an object to be tracked that affects the weighting of a GLBP gateway.

vrrp

To create a Virtual Router Redundancy Protocol version 3 (VRRPv3) group and enter VRRPv3 group configuration mode, use the **vrrp**. To remove the VRRPv3 group, use the **no** form of this command.

```
vrrp group-id address-family {ipv4 | ipv6}
no vrrp group-id address-family {ipv4 | ipv6}
```

Syntax Description		
	<i>group-id</i>	Virtual router group number. The range is from 1 to 255.
	address-family	Specifies the address-family for this VRRP group.
	ipv4	(Optional) Specifies IPv4 address.
	ipv6	(Optional) Specifies IPv6 address.

Command Default None

Command Modes Interface configuration (config-if)

Usage Guidelines

Examples

The following example shows how to create a VRRPv3 group and enter VRRP configuration mode:

```
Device(config-if)# vrrp 3 address-family ipv4
```

Related Commands	Command	Description
	timers advertise	Sets the advertisement timer in milliseconds.

vrrp description

To assign a description to the Virtual Router Redundancy Protocol (VRRP) group, use the **vrrp description** command in interface configuration mode. To remove the description, use the **no** form of this command.

description *text*
no description

Syntax Description

<i>text</i>	Text (up to 80 characters) that describes the purpose or use of the group.
-------------	--

Command Default

There is no description of the VRRP group.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Examples

The following example enables VRRP. VRRP group 1 is described as Building A – Marketing and Administration.

```
Device(config-if-vrrp)# description Building A - Marketing and Administration
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

vrrp preempt

To configure the device to take over as master virtual router for a Virtual Router Redundancy Protocol (VRRP) group if it has higher priority than the current master virtual router, use the **preempt** command in VRRP configuration mode. To disable this function, use the **no** form of this command.

preempt [**delay minimum** *seconds*]
no preempt

Syntax Description	delay minimum <i>seconds</i>	(Optional) Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.
---------------------------	-------------------------------------	--

Command Default This command is enabled.

Command Modes VRRP configuration (config-if-vrrp)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines By default, the device being configured with this command will take over as master virtual router for the group if it has a higher priority than the current master virtual router. You can configure a delay, which will cause the VRRP device to wait the specified number of seconds before issuing an advertisement claiming master ownership.



Note The device that is the IP address owner will preempt, regardless of the setting of this command.

Examples

The following example configures the device to preempt the current master virtual router when its priority of 200 is higher than that of the current master virtual router. If the device preempts the current master virtual router, it waits 15 seconds before issuing an advertisement claiming it is the master virtual router.

```
Device(config-if-vrrp)#preempt delay minimum 15
```

Related Commands	Command	Description
	vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
	priority	Sets the priority level of the device within a VRRP group.

vrrp priority

To set the priority level of the device within a Virtual Router Redundancy Protocol (VRRP) group, use the **priority** command in interface configuration mode. To remove the priority level of the device, use the **no** form of this command.

priority *level*
no priority *level*

Syntax Description

<i>level</i>	Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.
--------------	---

Command Default

The priority level is set to the default value of 100.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines

Use this command to control which device becomes the master virtual router.

Examples

The following example configures the device with a priority of 254:

```
Device(config-if-vrrp)# priority 254
```

Related Commands

Command	Description
vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.
vrrp preempt	Configures the device to take over as master virtual router for a VRRP group if it has higher priority than the current master virtual router.

vrrp timers advertise

To configure the interval between successive advertisements by the master virtual router in a Virtual Router Redundancy Protocol (VRRP) group, use the **timers advertise** command in VRRP configuration mode. To restore the default value, use the **no** form of this command.

timers advertise [**msec**] *interval*
no timers advertise [**msec**] *interval*

Syntax Description	
<i>group</i>	Virtual router group number. The group number range is from 1 to 255.
msec	(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.
<i>interval</i>	Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the msec keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the msec keyword is specified, the valid range is 50 to 999 milliseconds.

Command Default The default interval of 1 second is configured.

Command Modes VRRP configuration (config-if-vrrp)

Command History	Release	Modification
	Cisco IOS XE Release 2.1	This command was introduced.

Usage Guidelines The advertisements being sent by the master virtual router communicate the state and priority of the current master virtual router.

The **vrrp timers advertise** command configures the time between successive advertisement packets and the time before other routers declare the master router to be down. Routers or access servers on which timer values are not configured can learn timer values from the master router. The timers configured on the master router always override any other timer settings. All routers in a VRRP group must use the same timer values. If the same timer values are not set, the devices in the VRRP group will not communicate with each other and any misconfigured device will change its state to master.

Examples

The following example shows how to configure the master virtual router to send advertisements every 4 seconds:

```
Device(config-if-vrrp)# timers advertise 4
```

Related Commands	Command	Description
	vrrp	Creates a VRRPv3 group and enters VRRPv3 group configuration mode.

Command	Description
timers learn	Configures the device, when it is acting as backup virtual router for a VRRP group, to learn the advertisement interval used by the master virtual router.

vrrs leader

To specify a leader's name to be registered with Virtual Router Redundancy Service (VRRS), use the **vrrs leader** command. To remove the specified VRRS leader, use the **no** form of this command.

vrrs leader *vrrs-leader-name*
no vrrs leader *vrrs-leader-name*

Syntax Description

<i>vrrs-leader-name</i>	Name of VRRS Tag to lead.
-------------------------	---------------------------

Command Default

A registered VRRS name is unavailable by default.

Command Modes

VRRP configuration (config-if-vrrp)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example specifies a leader's name to be registered with VRRS:

```
Device(config-if-vrrp)# vrrs leader leader-1
```

Related Commands

Command	Description
vrrp	Creates a VRRP group and enters VRRP configuration mode.



PART **IV**

IP Multicast Routing

- [IP Multicast Routing, on page 209](#)



IP Multicast Routing

- [cache-memory-max](#), on page 211
- [clear ip mfib counters](#), on page 212
- [clear ip mroute](#), on page 213
- [ip igmp filter](#), on page 214
- [ip igmp max-groups](#), on page 215
- [ip igmp profile](#), on page 217
- [ip igmp snooping](#), on page 218
- [ip igmp snooping last-member-query-count](#), on page 219
- [ip igmp snooping querier](#), on page 221
- [ip igmp snooping report-suppression](#), on page 223
- [ip igmp snooping vlan mrouter](#), on page 224
- [ip igmp snooping vlan static](#), on page 225
- [ip multicast auto-enable](#), on page 226
- [ip pim accept-register](#), on page 227
- [ip pim bsr-candidate](#), on page 228
- [ip pim rp-candidate](#), on page 230
- [ip pim send-rp-announce](#), on page 231
- [ip pim spt-threshold](#), on page 233
- [match message-type](#), on page 234
- [match service-type](#), on page 235
- [match service-instance](#), on page 236
- [mrinfo](#), on page 237
- [redistribute mdns-sd](#), on page 239
- [service-list mdns-sd](#), on page 240
- [service-policy-query](#), on page 241
- [service-routing mdns-sd](#), on page 242
- [service-policy](#), on page 243
- [show ip igmp filter](#), on page 244
- [show ip igmp profile](#), on page 245
- [show ip igmp snooping](#), on page 246
- [show ip igmp snooping groups](#), on page 248
- [show ip igmp snooping mrouter](#), on page 250
- [show ip igmp snooping querier](#), on page 251

- [show ip pim autorp](#), on page 253
- [show ip pim bsr-router](#), on page 254
- [show ip pim bsr](#), on page 255
- [show ip pim tunnel](#), on page 256
- [show mdns cache](#), on page 258
- [show mdns requests](#), on page 260
- [show mdns statistics](#), on page 261
- [show platform software fed switch ip multicast](#), on page 262

cache-memory-max

To set the percentage of the system memory for cache, use the **cache-memory-max** command. To remove the percentage of system memory for cache, use the **no** form of this command.

cache-memory-max *cache-config-percentage*
no cache-memory-max *cache-config-percentage*

Syntax Description *cache-config-percentage* A percentage of the system memory for cache.

Command Default By default, the system memory is set to 10 percent.

Command Modes mDNS configuration

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

Usage Guidelines The number of services learned in a network could be large, so there is an upper limit on the amount of cache memory that can be used.



Note You can override the default value by using this command.

When you try to add new records, and the cache is full, the records in the cache that are close to expiring are deleted to provide space for the new records.

Example

This example sets 20 percent of the system memory for cache:

```
Device(config-mdns)# cache-memory-max 20
```

clear ip mfib counters

To clear all the active IPv4 Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ip mfib counters** command in privileged EXEC mode.

```
clear ip mfib [global | vrf *] counters [group-address] [hostname | source-address]
```

Syntax Description	
global	(Optional) Resets the IP MFIB cache to the global default configuration.
vrf *	(Optional) Clears the IP MFIB cache for all VPN routing and forwarding instances.
<i>group-address</i>	(Optional) Limits the active MFIB traffic counters to the indicated group address.
<i>hostname</i>	(Optional) Limits the active MFIB traffic counters to the indicated host name.
<i>source-address</i>	(Optional) Limits the active MFIB traffic counters to the indicated source address.

Command Default None

Command Modes Privileged EXEC (#)

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

Example

The following example shows how to reset all the active MFIB traffic counters for all the multicast tables:

```
Device# clear ip mfib counters
```

The following example shows how to reset the IP MFIB cache counters to the global default configuration:

```
Device# clear ip mfib global counters
```

The following example shows how to clear the IP MFIB cache for all the VPN routing and forwarding instances:

```
Device# clear ip mfib vrf * counters
```

clear ip mroute

To delete the entries in the IP multicast routing table, use the **clear ip mroute** command in privileged EXEC mode.

```
clear ip mroute [vrf vrf-name] { * | ip-address | group-address } [hostname | source-address]
```

Syntax Description		
vrf <i>vrf-name</i>	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.	
*	Specifies all Multicast routes.	
<i>ip-address</i>	Multicast routes for the IP address.	
<i>group-address</i>	Multicast routes for the group address.	
<i>hostname</i>	(Optional) Multicast routes for the host name.	
<i>source-address</i>	(Optional) Multicast routes for the source address.	

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines The *group-address* variable specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a group name or address, you can also enter the source argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Example

The following example shows how to delete all the entries from the IP multicast routing table:

```
Device# clear ip mroute *
```

The following example shows how to delete all the sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources:

```
Device# clear ip mroute 224.2.205.42 228.3.0.0
```

ip igmp filter

To control whether or not all the hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface, use the **ip igmp filter** interface configuration command on the device stack or on a standalone device. To remove the specified profile from the interface, use the **no** form of this command.

ip igmp filter *profile number*
no ip igmp filter

Syntax Description	<i>profile number</i> IGMP profile number to be applied. The range is 1—4294967295.
---------------------------	---

Command Default	No IGMP filters are applied.
------------------------	------------------------------

Command Modes	Interface configuration (config-if)
----------------------	-------------------------------------

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

Usage Guidelines	You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.
-------------------------	---

An IGMP profile can be applied to one or more device port interfaces, but one port can have only one profile applied to it.

Example

This example shows how to configure IGMP profile 40 to permit the specified range of IP multicast addresses, then shows how to apply that profile to a port as a filter:

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
Device(config-igmp-profile)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport
*Jan 3 18:04:17.007: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down.
NOTE: If this message appears, this interface changes to layer 2, so that you can apply the
filter.
Device(config-if)# ip igmp filter 40
```

You can verify your setting by using the **show running-config** command in privileged EXEC mode and by specifying an interface.

ip igmp max-groups

To set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table, use the **ip igmp max-groups** interface configuration command on the device stack or on a standalone device. To set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report, use the **no** form of this command.

```
ip igmp max-groups {max number | action { deny | replace }}
no ip igmp max-groups {max number | action }
```

Syntax Description

<i>max number</i>	Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.
action deny	Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.
action replace	Replaces the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the IGMP snooping forwarding table.

Command Default

The default maximum number of groups is no limit.

After the device learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for routed ports, switch virtual interfaces (SVIs), or ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as deny, and set the maximum group limit, the entries that were previously in the forwarding table are not removed, but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the device drops the next IGMP report received on the interface.
- If you configure the throttling action as replace, and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the device replaces a randomly selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups {deny | replace}** command has no effect.

Example

The following example shows how to limit the number of IGMP groups that a port can join to 25:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# ip igmp max-groups 25
```

The following example shows how to configure the device to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

ip igmp profile

To create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode, use the **ip igmp profile** global configuration command on the device stack or on a standalone device. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switch port. To delete the IGMP profile, use the **no** form of this command.

```
ip igmp profile profile number
no ip igmp profile profile number
```

Syntax Description

profile number The IGMP profile number being configured. The range is from 1—4294967295.

Command Default

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

Command Modes

Global configuration

Command History

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

Usage Guidelines

When you are in IGMP profile configuration mode, you can create a profile by using these commands:

- **deny**—Specifies that matching addresses are denied; this is the default condition.
- **exit**—Exits from igmp-profile configuration mode.
- **no**—Negates a command or resets to its defaults.
- **permit**—Specifies that matching addresses are permitted.
- **range**—Specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

Example

The following example shows how to configure IGMP profile 40, which permits the specified range of IP multicast addresses:

```
Device(config)# ip igmp profile 40
Device(config-igmp-profile)# permit
Device(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** command in privileged EXEC mode.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping on the device or to enable it on a per-VLAN basis, use the **ip igmp snooping** global configuration command on the device stack or on a standalone device. To return to the default setting, use the **no** form of this command.

ip igmp snooping [**vlan** *vlan-id*]

no ip igmp snooping [**vlan** *vlan-id*]

Syntax Description	vlan <i>vlan-id</i> (Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
Command Default	IGMP snooping is globally enabled on the device. IGMP snooping is enabled on VLAN interfaces.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all of the existing VLAN interfaces. When IGMP snooping is globally disabled, it is disabled on all of the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable IGMP snooping:

```
Device(config)# ip igmp snooping
```

The following example shows how to enable IGMP snooping on VLAN 1:

```
Device(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping last-member-query-count

To configure how often Internet Group Management Protocol (IGMP) snooping will send query messages in response to receiving an IGMP leave message, use the **ip igmp snooping last-member-query-count** command in global configuration mode. To set *count* to the default value, use the **no** form of this command.

```
ip igmp snooping [vlan vlan-id] last-member-query-count count
no ip igmp snooping [vlan vlan-id] last-member-query-count count
```

Syntax Description	vlan <i>vlan-id</i> (Optional) Sets the count value on a specific VLAN ID. The range is from 1—1001. Do not enter leading zeroes.	
	<i>count</i> Interval at which query messages are sent, in milliseconds. The range is from 1—7. The default is 2.	
Command Default	A query is sent every 2 milliseconds.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines When a multicast host leaves a group, the host sends an IGMP leave message. To check if this host is the last to leave the group, IGMP query messages are sent when the leave message is seen until the **last-member-query-interval** timeout period expires. If no response is received to the last-member queries before the timeout period expires, the group record is deleted.

Use the **ip igmp snooping last-member-query-interval** command to configure the timeout period.

When both IGMP snooping immediate-leave processing and the query count are configured, immediate-leave processing takes precedence.



Note Do not set the count to 1 because the loss of a single packet (the query packet from the device to the host or the report packet from the host to the device) may result in traffic forwarding being stopped even if the receiver is still there. Traffic continues to be forwarded after the next general query is sent by the device, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to 1 last-member query interval (LMQI) value when the device is processing more than one leave within an LMQI. In such a scenario, the average leave latency is determined by the $(\text{count} + 0.5) * \text{LMQI}$. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

Example

The following example shows how to set the last member query count to 5:

```
Device(config)# ip igmp snooping last-member-query-count 5
```

ip igmp snooping querier

To globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks, use the **ip igmp snooping querier** global configuration command. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. To return to the default settings, use the **no** form of this command.

```
ip igmp snooping [vlan vlan-id] querier [address ip-address | max-response-time response-time
| query-interval interval-count | tcn query {count count | interval interval} | timer expiry
expiry-time | version version]
no ip igmp snooping [vlan vlan-id] querier [address | max-response-time | query-interval |
tcn query {count | interval} | timer expiry | version]
```

Syntax Description		
vlan <i>vlan-id</i>	(Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1—1001 and 1006—4094.	
address <i>ip-address</i>	(Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.	
max-response-time <i>response-time</i>	(Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1—25 seconds.	
query-interval <i>interval-count</i>	(Optional) Sets the interval between IGMP queriers. The range is 1—18000 seconds.	
tcn query	(Optional) Sets parameters related to Topology Change Notifications (TCNs).	
count <i>count</i>	Sets the number of TCN queries to be executed during the TCN interval time. The range is 1—10.	
interval <i>interval</i>	Sets the TCN query interval time. The range is 1—255.	
timer expiry <i>expiry-time</i>	(Optional) Sets the length of time until the IGMP querier expires. The range is 60—300 seconds.	
version <i>version</i>	(Optional) Selects the IGMP version number that the querier feature uses. Select either 1 or 2.	

Command Default The IGMP snooping querier feature is globally disabled on the device. When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast router.

Command Modes Global configuration

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

Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a querier.

By default, the IGMP snooping querier is configured to detect devices that use IGMP Version 2 (IGMPv2), but does not detect clients that are using IGMP Version 1 (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the max-response-time when devices use IGMPv1. (The value cannot be configured, and is set to zero).

Non-RFC-compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

Example

The following example shows how to globally enable the IGMP snooping querier feature:

```
Device(config)# ip igmp snooping querier
```

The following example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Device(config)# ip igmp snooping querier max-response-time 25
```

The following example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Device(config)# ip igmp snooping querier query-interval 60
```

The following example shows how to set the IGMP snooping querier TCN query count to 25:

```
Device(config)# ip igmp snooping querier tcn count 25
```

The following example shows how to set the IGMP snooping querier timeout value to 60 seconds:

```
Device(config)# ip igmp snooping querier timer expiry 60
```

The following example shows how to set the IGMP snooping querier feature to Version 2:

```
Device(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping report-suppression

To enable Internet Group Management Protocol (IGMP) report suppression, use the **ip igmp snooping report-suppression** global configuration command on the device stack or on a standalone device. To disable IGMP report suppression, and to forward all IGMP reports to multicast routers, use the **no** form of this command.

ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Syntax Description This command has no arguments or keywords.

Command Default IGMP report suppression is enabled.

Command Modes Global configuration

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

Usage Guidelines IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The device uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP report suppression is enabled (the default), the device sends the first IGMP report from all the hosts for a group to all the multicast routers. The device does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the device forwards only the first IGMPv1 or IGMPv2 report from all the hosts for a group to all of the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the device forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all of the multicast routers.

Example

The following example shows how to disable report suppression:

```
Device(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip igmp snooping vlan mrouter

To add a multicast router port, use the **ip igmp snooping mrouter** global configuration command on the device stack or on a standalone device. To return to the default settings, use the **no** form of this command.

```
ip igmp snooping vlan vlan-id mrouter {interface interface-id}
no ip igmp snooping vlan vlan-id mrouter {interface interface-id}
```

Syntax Description	<i>vlan-id</i>	Enables IGMP snooping, and adds the port in the specified VLAN as the multicast router port. Ranges are 1—1001 and 1006—4094.
	interface <i>interface-id</i>	Specifies the next-hop interface to the multicast router. The arguments have these meanings: <ul style="list-style-type: none"> • <i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface. • <i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface. • <i>port-channel interface number</i>—A channel interface. The range is 0—128.

Command Default By default, there are no multicast router ports.

Command Modes Global configuration

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

Usage Guidelines VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping. The configuration is saved in NVRAM.

Example

The following example shows how to configure a port as a multicast router port:

```
Device(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet1/0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

ip igmp snooping vlan static

To enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** global configuration command on the device stack or on a standalone device. To remove the port specified as members of a static multicast group, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*
no ip igmp snooping vlan *vlan-id* **static** *ip-address* **interface** *interface-id*

Syntax Description

<i>vlan-id</i>	Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.
<i>ip-address</i>	Adds a Layer 2 port as a member of a multicast group with the specified group IP address.
interface <i>interface-id</i>	Specifies the interface of the member port. The <i>interface-id</i> has these options: <ul style="list-style-type: none"> • <i>fastethernet interface number</i>—A Fast Ethernet IEEE 802.3 interface. • <i>gigabitethernet interface number</i>—A Gigabit Ethernet IEEE 802.3z interface. • <i>tengigabitethernet interface number</i>—A 10-Gigabit Ethernet IEEE 802.3z interface. • <i>port-channel interface number</i>—A channel interface. The range is 0—128.

Command Default

By default, no ports are statically configured as members of a multicast group.

Command Modes

Global configuration

Command History

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

Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

Example

The following example shows how to statically configure a host on an interface:

```
Device(config)# ip igmp snooping vlan 1 static 224.2.4.12 interface
gigabitEthernet1/0/1
```

Configuring port gigabitethernet1/0/1 on group 224.2.4.12

You can verify your settings by entering the **show ip igmp snooping** command in privileged EXEC mode.

ip multicast auto-enable

To support authentication, authorization, and accounting (AAA) enabling of IP multicast, use the **ip multicast auto-enable** command. This command allows multicast routing to be enabled dynamically on dialup interfaces using AAA attributes from a RADIUS server. To disable IP multicast for AAA, use the **no** form of this command.

ip multicast auto-enable
no ip multicast auto-enable

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Global configuration

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

Usage Guidelines None

Example

The following example shows how to enable AAA on IP multicast:

```
Device(config)# ip multicast auto-enable
```

ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To disable this function, use the **no** form of this command.

```
ip pim [vrf vrf-name ] accept-register {list access-list}
no ip pim [vrf vrf-name ] accept-register
```

Syntax Description	<p>vrf <i>vrf-name</i> (Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.</p> <p>list <i>access-list</i> Specifies the <i>access-list</i> argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100—199 and the expanded range is 2000—2699. An IP-named access list can also be used.</p>	
Command Default	No PIM register filters are configured.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list provided for the **ip pim accept-register** command should only filter IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is required, use the **ip multicast boundary** command instead.

Example

The following example shows how to permit register packets for a source address sending to any group range, with the exception of source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). These are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first-hop routers or switches.

```
Device(config)# ip pim accept-register list ssm-range
Device(config)# ip access-list extended ssm-range
Device(config-ext-nacl)# deny ip any 232.0.0.0 0.255.255.255
Device(config-ext-nacl)# permit ip any any
```

ip pim bsr-candidate

To configure the Device to be a candidate BSR, use the **ip pim bsr-candidate** command in global configuration mode. To remove the switch as a candidate BSR, use the **no** form of this command.

```
ip pim [vrf vrf-name] bsr-candidate interface-id [hash-mask-length] [priority]  
no ip pim [vrf vrf-name] bsr-candidate
```

Syntax Description	
vrf <i>vrf-name</i>	(Optional) Configures the Device to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
<i>interface-id</i>	ID of the interface on the Device from which the BSR address is derived to make it a candidate. This interface must be enabled for Protocol Independent Multicast (PIM) using the ip pim command. Valid interfaces include physical ports, port channels, and VLANs.
<i>hash-mask-length</i>	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
<i>priority</i>	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.

Command Default The Device is not configured to announce itself as a candidate BSR.

Command Modes Global configuration

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

Usage Guidelines

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command configures the Device to send BSR messages to all of its PIM neighbors, with the address of the designated interface as the BSR address.

This command should be configured on backbone Devices that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) switches unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so, no pre-existing IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each switch that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Cisco Device always accept and process BSR messages. There is no command to disable this function.

Cisco Device perform the following steps to determine which C-RP is used for a group:

- A long match lookup is performed on the group prefix that is announced by the BSR C-RPs.
- If more than one BSR-learned C-RP is found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
- If more than one BSR-learned C-RP has the same priority, the BSR hash function is used to select the RP for a group.
- If more than one BSR-learned C-RP returns the same hash value derived from the BSR hash function, the BSR C-RP with the highest IP address is preferred.

Example

The following example shows how to configure the IP address of the Device on Gigabit Ethernet interface 1/0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
Device(config)# ip pim bsr-candidate GigabitEthernet1/0/1 0 192
```

ip pim rp-candidate

To configure the Device to advertise itself to the BSR as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove the Device as a C-RP, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
no ip pim [vrf vrf-name] rp-candidate interface-id [group-list access-list-number]
```

Syntax Description		
	vrf <i>vrf-name</i>	(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
	<i>interface-id</i>	ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.
	group-list <i>access-list-number</i>	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.

Command Default The Device is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes Global configuration

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

Usage Guidelines Use this command to configure the Device to send PIMv2 messages so that it advertises itself as a candidate RP to the BSR.

This command should be configured on backbone Devices that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified by *interface-id* will be advertised as the C-RP address.

The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list-number* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.

Example

The following example shows how to configure the switch to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 1/0/1.

```
Device(config)# ip pim rp-candidate GigabitEthernet1/0/1 group-list 4
```

ip pim send-rp-announce

To use Auto-RP to configure groups for which the Device will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure the Device as an RP, use the **no** form of this command.

```
ip pim [vrf vrf-name] send-rp-announce interface-id scope ttl-value [group-list access-list-number]
[interval seconds]
```

```
no ip pim [vrf vrf-name] send-rp-announce interface-id
```

Syntax Description

vrf <i>vrf-name</i>	(Optional) Uses Auto-RP to configure groups for which the Device will act as a rendezvous point (RP) for the <i>vrf-name</i> argument.
<i>interface-id</i>	Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.
scope <i>ttl-value</i>	Specifies the time-to-live (TTL) value in hops that limits the number of Auto-RP announcements. Enter a hop count that is high enough to ensure that the RP-announce messages reach all the mapping agents in the network. There is no default setting. The range is 1—255.
group-list <i>access-list-number</i>	(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address. Enter an IP standard access list number from 1—99. If no access list is configured, the RP is used for all groups.
interval <i>seconds</i>	(Optional) Specifies the interval between RP announcements, in seconds. The total hold time of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds. The range is 1—16383.

Command Default

Auto-RP is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Enter this command on the Device that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39). This message announces the router as a candidate RP for the groups in the range described by the access list.

Example

The following example shows how to configure the Device to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the switch wants to be identified as RP is the IP address associated with Gigabit Ethernet interface 1/0/1 at an interval of 120 seconds:

ip pim send-rp-announce

```
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval  
120
```


ip pim spt-threshold

To specify the threshold that must be reached before moving to shortest-path tree (spt), use the **ip pim spt-threshold** command in global configuration mode. To remove the threshold, use the **no** form of this command.

```
ip pim {kpbs | infinity} [group-list access-list]
no ip pim {kpbs | infinity} [group-list access-list]
```

Syntax Description	<i>kpbs</i>	Threshold that must be reached before moving to shortest-path tree (spt). 0 is the only valid entry even though the range is 0 to 4294967. A 0 entry always switches to the source-tree.
	infinity	Specifies that all the sources for the specified group use the shared tree, never switching to the source tree.
	group-list access-list	(Optional) Specifies an access list number or a specific access list that you have created by name. If the value is 0 or if the group-list access-list option is not used, the threshold applies to all the groups.
Command Default	Switches to the PIM shortest-path tree (spt).	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Example

The following example shows how to make all the sources for access list 16 use the shared tree:

```
Device(config)# ip pim spt-threshold infinity group-list 16
```

match message-type

To set a message type to match a service list, use the **match message-type** command.

```
match message-type {announcement | any | query}
```

Syntax Description

announcement	Allows only service advertisements or announcements for the Device.
any	Allows any match type.
query	Allows only a query from the client for a certain Device in the network.

Command Default

None

Command Modes

Service list configuration.

Command History

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

Usage Guidelines

Multiple service maps of the same name with different sequence numbers can be created, and the evaluation of the filters will be ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each one having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is stopped once the first statement match is found and a permit/deny action associated with the statement match is performed. The default action after scanning through the entire list is to deny.



Note

It is not possible to use the **match** command if you have used the **service-list mdns-sd service-list-name query** command. The **match** command can be used only for the **permit** or **deny** option.

Example

The following example shows how to set the announcement message type to be matched:

```
Device(config-mdns-sd-sl) # match message-type announcement
```

match service-type

To set the value of the mDNS service type string to match, use the **match service-type** command.

match service-type *line*

Syntax Description	<i>line</i> Regular expression to match the service type in packets.				
Command Default	None				
Command Modes	Service list configuration				
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.				
Usage Guidelines	It is not possible to use the match command if you have used the service-list mdns-sd service-list-name query command. The match command can be used only for the permit or deny option.				

Example

The following example shows how to set the value of the mDNS service type string to match:

```
Device(config-mdns-sd-sl)# match service-type _ipp._tcp
```

match service-instance

To set a service instance to match a service list, use the **match service-instance** command.

match service-instance *line*

Syntax Description	<i>line</i> Regular expression to match the service instance in packets.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Service list configuration
----------------------	----------------------------

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

Usage Guidelines	It is not possible to use the match command if you have used the service-list mdns-sd service-list-name query command. The match command can be used only for the permit or deny option.
-------------------------	---

Example

The following example shows how to set the service instance to match:

```
Device(config-mdns-sd-sl)# match service-instance servInst 1
```

mrinfo

To query which neighboring multicast routers or multilayer switches are acting as peers, use the **mrinfo** command in user EXEC or privileged EXEC mode.

mrinfo [*vrf route-name*] [*hostname | address*] [*interface-id*]

Syntax Description	
<i>vrf route-name</i>	(Optional) Specifies the VPN routing or forwarding instance.
<i>hostname address</i>	(Optional) Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
<i>interface-id</i>	(Optional) Interface ID.

Command Default The command is disabled.

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers or switches are peering with multicast routers or switches. Cisco routers supports **mrinfo** requests from Cisco IOS Release 10.2.

You can query a multicast router or multilayer switch using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Example

The following is the sample output from the **mrinfo** command:

```
Device# mrinfo
vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```



Note The flags indicate the following:

- P: prune-capable
 - M: mtrace-capable
 - S: Simple Network Management Protocol-capable
 - A: Auto RP capable
-

redistribute mdns-sd

To redistribute services or service announcements across subnets, use the **redistribute mdns-sd** command. To disable redistribution of services or service announcements across subnets, use the **no** form of this command.

redistribute mdns-sd
no redistribute mdns-sd

This command has no arguments or keywords.

Command Default

The redistribution of services or service announcements across subnets is disabled.

Command Modes

mDNS configuration

Command History

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

Usage Guidelines

To redistribute service announcements across interfaces, use the **redistribute mdns-sd** command. This command sends out unsolicited announcements received on one interface to all of the other interfaces. The outgoing announcements are filtered as per the out-service policy defined for the interface, or, in absence of a per-interface service policy, based on the global out-service policy.

In the absence of a redistribute option, services can be discovered by querying in a Layer 3 domain that is not local to the service provider.

Example

The following example shows how to redistribute services or service announcements across subnets:

```
Device(config-mdns)# redistribute mdns-sd
```



Note If redistribution is enabled globally, global configuration is given higher priority than interface configuration.

service-list mdns-sd

To enter mDNS service discovery service-list mode on the device, use the **service-list mdns-sd** command. To exit mDNS service discovery service-list mode, use the **no** form of this command.

service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]
no service-list mdns-sd *service-list-name* {**permit** | **deny**} *sequence-number* [**query**]

Syntax Description		
	<i>service-list-name</i>	Name of the service list.
	permit <i>sequence number</i>	Permits a filter on the service list to be applied to the sequence number.
	deny <i>sequence number</i>	Denies a filter on the service list to be applied to the sequence number.
	query	Associates a query for the service list name.

Command Default Disabled.

Command Modes Global configuration

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

Usage Guidelines Service filters are modeled around access lists and route maps.

Multiple service maps of the same name with different sequence numbers can be created and the evaluation of the filters ordered on the sequence number. Service lists are an ordered sequence of individual statements, with each having a permit or deny result. The evaluation of a service list consists of a list scan in a predetermined order, and an evaluation of the criteria of each statement that matches. A list scan is terminated once the first statement match is found, and an action, permit, or deny that is associated with the statement match is performed. The default action after scanning through the entire list will be to deny.

This command can be used to enter mDNS service discovery service-list mode.

In this mode you can:

- Create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to the sequence number.

Example

The following example shows how to create a service list and apply a filter on the service list according to the **permit** or **deny** option applied to a sequence number:

```
Device(config)# service-list mdns-sd s11 permit 3
```


service-policy-query

To configure the service-list query periodicity, use the **service-policy-query** command. To delete the configuration, use the **no** form of this command.

service-policy-query [*service-list-query-name service-list-query-periodicity*]
no service-policy-query

Syntax Description	<i>service-list-query-name service-list-query-periodicity</i> (Optional) Service-list query periodicity.
---------------------------	--

Command Default	Disabled.
------------------------	-----------

Command Modes	mDNS configuration
----------------------	--------------------

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

Usage Guidelines	Since there are devices that do not send unsolicited announcements and to force such devices the learning of services and to keep them refreshed in the cache, this command contains an active query feature that ensures that the services listed in the active query list are queried.
-------------------------	--

Example

This example shows how to configure service list query periodicity:

```
Device(config-mdns)# service-policy-query sl-query1 100
```

service-routing mdns-sd

To enable the mDNS gateway functionality for a device and enter multicast DNS configuration mode, use the **service-routing mdns-sd** command. To restore the default settings and return to global configuration mode, enter the **no** form of this command.

service-routing mdns-sd
no service-routing mdns-sd

This command has no arguments or keywords.

Command Default Disabled.

Command Modes Global configuration

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

Usage Guidelines The mDNS gateway functionality can only be enabled or disabled globally, not on a per-interface basis. The service- filter policy and redistribution can be configured globally as well as on a per-interface basis. Any interface-specific configuration overrides the global configuration.

Example

The following example shows how to enable the mDNS gateway functionality for a device and enter multicast DNS configuration mode:

```
Device (config) # service-routing mdns-sd
```

service-policy

To apply a filter on incoming or outgoing service-discovery information on a service list, use the **service-policy** command. To remove the filter, use the **no** form of this command.

```
service-policy service-policy-name {IN | OUT}
no service-policy service-policy-name {IN | OUT}
```

Syntax Description	IN Applies a filter on incoming service-discovery information.	
	OUT Applies a filter on outgoing service-discovery information.	
Command Default	Disabled.	
Command Modes	mDNS configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Example

The following example shows how to apply a filter on incoming service-discovery information on a service list:

```
Device(config-mdns)# service-policy serv-poll IN
```

show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the **show ip igmp filter** command in privileged EXEC mode.

show ip igmp [*vrf vrf-name*] **filter**

Syntax Description	<i>vrf vrf-name</i> (Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
---------------------------	--

Command Default	IGMP filters are enabled by default.
------------------------	--------------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

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

Usage Guidelines	The show ip igmp filter command displays information about all filters defined on the device.
-------------------------	--

Example

The following example shows the sample output from the **show ip igmp filter** command:

```
Device# show ip igmp filter
IGMP filter enabled
```

show ip igmp profile

To display all the configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile, use the **show ip igmp profile** command in privileged EXEC mode.

```
show ip igmp [vrf vrf-name] profile [profile number]
```

Syntax Description	vrf vrf-name (Optional) Supports the multicast VPN routing and forwarding (VRF) instance.	
	profile number (Optional) IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all the IGMP profiles are displayed.	
Command Default	IGMP profiles are undefined by default.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
Usage Guidelines	None	

Examples

The following example shows the output of the **show ip igmp profile** command for profile number 40 on the device:

```
Device# show ip igmp profile 40
IGMP Profile 40
  permit
  range 233.1.1.1 233.255.255.255
```

The following example shows the output of the **show ip igmp profile** command for all the profiles configured on the device:

```
Device# show ip igmp profile

IGMP Profile 3
  range 230.9.9.0 230.9.9.0
IGMP Profile 4
  permit
  range 229.9.9.0 229.255.255.255
```

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of the device or the VLAN, use the **show ip igmp snooping** command in user EXEC or privileged EXEC mode.

show ip igmp snooping [**groups** | **mrouter** | **querier**] [**vlan** *vlan-id*] [**detail**]

Syntax Description	
groups	(Optional) Displays the IGMP snooping multicast table.
mrouter	(Optional) Displays the IGMP snooping multicast router ports.
querier	(Optional) Displays the configuration and operation information for the IGMP querier.
vlan <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
detail	(Optional) Displays operational state information.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping. Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Examples

The following is a sample output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN:

```
Device# show ip igmp snooping vlan 1

Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
-----
IGMP snooping                : Enabled
```

```

IGMPv2 immediate leave      : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode   : IGMP_ONLY
Robustness variable         : 2
Last member query count      : 2
Last member query interval   : 1000

```

The following is a sample output from the **show ip igmp snooping** command. It displays snooping characteristics for all the VLANs on the device:

```

Device# show ip igmp snooping

Global IGMP Snooping configuration:
-----
IGMP snooping                : Enabled
IGMPv3 snooping (minimal)    : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 1:
-----
IGMP snooping                : Enabled
IGMPv2 immediate leave      : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode   : IGMP_ONLY
Robustness variable         : 2
Last member query count      : 2
Last member query interval   : 1000
Vlan 2:
-----
IGMP snooping                : Enabled
IGMPv2 immediate leave      : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode   : IGMP_ONLY
Robustness variable         : 2
Last member query count      : 2
Last member query interval   : 1000
-
.
.
.

```

show ip igmp snooping groups

To display the Internet Group Management Protocol (IGMP) snooping multicast table for the device or the multicast information, use the **show ip igmp snooping groups** command in privileged EXEC mode.

show ip igmp snooping groups [*vlan vlan-id*] [[*count*] | *ip_address*]

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.
count	(Optional) Displays the total number of entries for the specified command options instead of the actual entries.
<i>ip_address</i>	(Optional) Characteristics of the multicast group with the specified group IP address.

Command Modes

Privileged EXEC
User EXEC

Command History

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

Usage Guidelines

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

Examples

The following is a sample output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the device.

```
Device# show ip igmp snooping groups
```

```
Vlan      Group          Type      Version      Port List
-----
1         224.1.4.4      igmp
1         224.1.4.5      igmp
2         224.0.1.40     igmp      v2           Gi1/0/15
104      224.1.4.2      igmp      v2           Gi2/0/1, Gi2/0/2
104      224.1.4.3      igmp      v2           Gi2/0/1, Gi2/0/2
```

The following is a sample output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the device.

```
Device# show ip igmp snooping groups count
```

```
Total number of multicast groups: 2
```

The following is a sample output from the **show ip igmp snooping groups vlan vlan-id ip-address** command. It shows the entries for the group with the specified IP address:

```
Device# show ip igmp snooping groups vlan 104 224.1.4.2
```

```
Vlan      Group          Type      Version      Port List
```



```
-----  
104      224.1.4.2      igmp      v2      Gi2/0/1, Gi1/0/15
```

show ip igmp snooping mrouter

To display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the device or for the specified multicast VLAN, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

show ip igmp snooping mrouter [*vlan* *vlan-id*]

Syntax Description	vlan <i>vlan-id</i> (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.	
Command Modes	User EXEC Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
Usage Guidelines	<p>VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.</p> <p>When multicast VLAN registration (MVR) is enabled, the show ip igmp snooping mrouter command displays MVR multicast router information and IGMP snooping information.</p> <p>Expressions are case sensitive, for example, if you enter exclude output, the lines that contain "output" do not appear, but the lines that contain "Output" appear.</p>	

Example

The following is a sample output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the device:

```
Device# show ip igmp snooping mrouter

Vlan      ports
----      -
  1       Gi2/0/1 (dynamic)
```

show ip igmp snooping querier

To display the configuration and operation information for the IGMP querier that is configured on a device, use the **show ip igmp snooping querier** command in user EXEC mode.

```
show ip igmp snooping querier [vlan vlan-id] [detail ]
```

Syntax Description	
vlan <i>vlan-id</i>	(Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.
detail	(Optional) Displays detailed IGMP querier information.

Command Modes	
	User EXEC
	Privileged EXEC

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

Usage Guidelines Use the **show ip igmp snooping querier** command to display the IGMP version and the IP address of a detected device, also called a querier, that sends IGMP query messages. A subnet can have multiple multicast routers but only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 device.

The **show ip igmp snooping querier** command output also shows the VLAN and the interface on which the querier was detected. If the querier is the device, the output shows the Port field as Router. If the querier is a router, the output shows the port number on which the querier was detected in the Port field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier** command displays only the device IP address most recently detected by the device querier.

The **show ip igmp snooping querier detail** command displays the device IP address most recently detected by the device querier and this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the device querier (if any) that is configured in the VLAN

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

Examples

The following is a sample output from the **show ip igmp snooping querier** command:

```
Device> show ip igmp snooping querier
Vlan      IP Address      IGMP Version      Port
-----
1         172.20.50.11   v3                 Gi1/0/1
2         172.20.40.20   v2                 Router
```

The following is a sample output from the **show ip igmp snooping querier detail** command:

```
Device> show ip igmp snooping querier detail

Vlan      IP Address      IGMP Version  Port
-----
1         1.1.1.1        v2            Fa8/0/1
Global IGMP device querier status

-----
admin state           : Enabled
admin version        : 2
source IP address     : 0.0.0.0
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count      : 2
tcn query interval (sec) : 10
Vlan 1:  IGMP device querier status

-----
elected querier is 1.1.1.1      on port Fa8/0/1
-----
admin state           : Enabled
admin version        : 2
source IP address     : 10.1.1.65
query-interval (sec) : 60
max-response-time (sec) : 10
querier-timeout (sec) : 120
tcn query count      : 2
tcn query interval (sec) : 10
operational state     : Non-Querier
operational version   : 2
tcn query pending count : 0
```

show ip pim autorp

To display global information about auto-rp, use the **show ip pim autorp** command in privileged EXEC mode.

show ip pim autorp

Syntax Description This command has no arguments or keywords.

Command Default Auto RP is enabled by default.

Command Modes Privileged EXEC

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

Usage Guidelines This command displays whether auto-rp is enabled or disabled.

Example

The following command output shows that Auto RP is enabled:

```
Device# show ip pim autorp

AutoRP Information:
  AutoRP is enabled.
  RP Discovery packet MTU is 0.
  224.0.1.40 is joined on GigabitEthernet1/0/1.

PIM AutoRP Statistics: Sent/Received
  RP Announce: 0/0, RP Discovery: 0/0
```

show ip pim bsr-router

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim bsr-router

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.

The following is sample output from the **show ip pim bsr-router** command:

```
Device# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim bsr

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the **show ip pim bsr** command in user EXEC or privileged EXEC mode.

show ip pim bsr

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines In addition to Auto RP, the BSR RP method can be configured. After the BSR RP method is configured, this command displays the BSR router information.

The following is sample output from the **show ip pim bsr** command:

```
Device# show ip pim bsr

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and decapsulation tunnels on an interface, use the **show ip pim tunnel** command.

show ip pim [**vrf** *vrf-name*] **tunnel** [**Tunnel** *interface-number* | **verbose**]

Syntax Description	vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
	Tunnel <i>interface-number</i>	(Optional) Specifies the tunnel interface number.
	verbose	(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

Use the **show ip pim tunnel** to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel)

The PIM Encap Tunnel is dynamically created whenever a group-to-rendezvous point (RP) mapping is learned (through auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop designated routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created—but it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.



Note PIM tunnels will not appear in the running configuration.

The following syslog message appears when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>,
changed state to up
```

The following is sample output from the **show ip pim tunnel** taken from an RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP:


```
Device# show ip pim tunnel
```

```
Tunnel0  
  Type : PIM Encap  
  RP   : 70.70.70.1*  
  Source: 70.70.70.1  
Tunnel1*  
  Type : PIM Decap  
  RP   : 70.70.70.1*  
  Source: -R2#
```



Note The asterisk (*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

show mdns cache

To display mDNS cache information for the device, use the **show mdns cache** command in privileged EXEC mode.

show mdns cache [**interface** *type number* | **name** *record-name* [**type** *record-type*] | **type** *record-type*]

Syntax Description	
interface <i>type-number</i>	(Optional) Specifies a particular interface type and number for which mDNS cache information is to be displayed.
name <i>record-name</i>	(Optional) Specifies a particular name for which mDNS cache information is to be displayed.
type <i>record-type</i>	(Optional) Specifies a particular type for which mDNS cache information is to be displayed.

Command Default None

Command Modes Privileged EXEC
User EXEC

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

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

Example

The following is an example of output from the **show mdns cache** command without any keywords:

```
Device# show mdns cache
```

```
[<NAME>]                [<TYPE>] [<CLASS>] [<TTL>/Remaining] [Accessed] [If-name] [Mac
Address] [<RR Record Data>]

 _airplay._tcp.local          PTR      IN      4500/4455      0      V1121
 b878.2e33.c7c5 CAMPUS APPLE TV1._airplay._tcp.local

 CAMPUS APPLE TV1._airplay._tcp.local SRV      IN      120/75      2      V1121
 b878.2e33.c7c5 CAMPUS-APPLE-TV1.local

 CAMPUS-APPLE-TV1.local      A        IN      120/75      2      V1121
 b878.2e33.c7c5 121.1.0.254

 CAMPUS APPLE TV1._airplay._tcp.local TXT      IN      4500/4455      2      V1121
 b878.2e33.c7c5 (162) 'deviceid=B8:78:2E:33:C7:C6'
```

```

'features=0x5a7ffff7''flags=0x4'
'model=AppleT~'~
_ipp._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._ipp._tcp.local
EPSON XP-400 Series._ipp._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local
EPSONC053AA.local A IN 120/85 2 V12
2894.0fed.447f 121.1.0.251
EPSON XP-400 Series._ipp._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (384)'txtvers=1' N XP-400 Series'
'usbFG=EPSON''usb_MDL=XP~'~
_smb._tcp.local PTR IN 4500/4465 2 V12
2894.0fed.447f EPSON XP-400 Series._smb._tcp.local
EPSON XP-400 Series._smb._tcp.local SRV IN 120/85 2 V12
2894.0fed.447f EPSONC053AA.local
EPSON XP-400 Series._smb._tcp.local TXT IN 4500/4465 2 V12
2894.0fed.447f (1)'' R2-Access1#

```

show mdns requests

To display information for outstanding mDNS requests, including record name and record type information, for the device, use the **show mdns requests** command in privileged EXEC mode.

show mdns requests [**detail** | **name** *record-name* | **type** *record-type* [**name** *record-name*]]

Syntax Description	detail	Displays detailed mDNS request information.
	name <i>record-name</i>	Displays detailed mDNS request information based on name.
	type <i>record-type</i>	Displays detailed mDNS request information based on type.

Command Default None

Command Modes Privileged EXEC
User EXEC

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

Usage Guidelines Expressions are case sensitive. For example, if you enter | exclude output, the lines that contain output do not appear, but the lines that contain output appear.

Example

This is an example of output from the **show mdns requests** command without any keywords:

```
Device# show mdns requests
MDNS Outstanding Requests
=====
Request name  :  _airplay._tcp.local
Request type  :  PTR
Request class :  IN
-----
Request name  :  *.*
Request type  :  PTR
Request class :  IN
```

show mdns statistics

To display mDNS statistics for the device, use the **show mdns statistics** command in privileged EXEC mode.

```
show mdns statistics { all | service-list list-name | service-policy { all | interface type-number } }
```

Syntax Description		
all		Displays the service policy, service list, and interface information.
service-list <i>list-name</i>		Displays the service list information.
service-policy		Displays the service policy information.
interface <i>type number</i>		Displays interface information.

Command Default None

Command Modes Privileged EXEC
User EXEC

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

Usage Guidelines Expressions are case sensitive, for example, if you enter | **exclude output**, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

Example

The following is a sample output from the **show mdns statistics all** command:

```
Device# show mdns statistics all

mDNS Statistics
mDNS packets sent      : 0
mDNS packets received  : 0
mDNS packets dropped   : 0
mDNS cache memory in use: 64224(bytes)
```

show platform software fed switch ip multicast

To display platform-dependent IP multicast tables and other information, use the **show platform software fed switch ip multicast** command in privileged EXEC mode.

show platform software fed switch {*switch-number* | **active** | **standby**} **ip multicast** {**groups** | **hardware** [{**detail**}] | **interfaces** | **retry**}

Syntax Description

switch { <i>switch_num</i> active standby }	The device for which you want to display information. <ul style="list-style-type: none"> • <i>switch_num</i>—Enter the switch ID. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available.
groups	Displays the IP multicast routes per group.
hardware [detail]	Displays the IP multicast routes loaded into hardware. The optional detail keyword is used to show the port members in the destination index and route index.
interfaces	Displays the IP multicast interfaces.
retry	Displays the IP multicast routes in the retry queue.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is not supported on switches running the LAN Base feature set.

Example

The following example shows how to display platform IP multicast routes per group:

```
Device# show platform software fed active ip multicast groups

Total Number of entries:3
MROUTE ENTRY vrf 0 (*, 224.0.0.0)
Token: 0x0000001f6 flags: C
No RPF interface.
Number of OIF: 0
Flags: 0x10 Pkts : 0
```

OIF Details:No OIF interface.

DI details

Handle:0x603cf7f8 Res-Type:ASIC_RSC_DI Asic-Num:255
 Feature-ID:AL_FID_L3_MULTICAST_IPV4_Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
 Hardware Indices/Handles: index0:0x51f6 index1:0x51f6

Cookie length 56

0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x4 0xe0 0x0 0x0 0x0 0x0 0x0
 0x0
 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0

Detailed Resource Information (ASIC# 0)

al_rsc_di

RM:index = 0x51f6
 RM:pmap = 0x0
 RM:cmi = 0x0
 RM:rcp_pmap = 0x0
 RM:force data copy = 0
 RM:remote cpu copy = 0
 RM:remote data copy = 0
 RM:local cpu copy = 0
 RM:local data copy = 0

al_rsc_cmi

RM:index = 0x51f6
 RM:cti_lo[0] = 0x0
 RM:cti_lo[1] = 0x0
 RM:cti_lo[2] = 0x0
 RM:cpu_q_vpn[0] = 0x0
 RM:cpu_q_vpn[1] = 0x0
 RM:cpu_q_vpn[2] = 0x0
 RM:npu_index = 0x0
 RM:strip_seg = 0x0
 RM:copy_seg = 0x0

Detailed Resource Information (ASIC# 1)

al_rsc_di

RM:index = 0x51f6
 RM:pmap = 0x0
 RM:cmi = 0x0
 RM:rcp_pmap = 0x0
 RM:force data copy = 0
 RM:remote cpu copy = 0
 RM:remote data copy = 0
 RM:local cpu copy = 0
 RM:local data copy = 0

al_rsc_cmi

RM:index = 0x51f6
 RM:cti_lo[0] = 0x0
 RM:cti_lo[1] = 0x0
 RM:cti_lo[2] = 0x0
 RM:cpu_q_vpn[0] = 0x0
 RM:cpu_q_vpn[1] = 0x0
 RM:cpu_q_vpn[2] = 0x0
 RM:npu_index = 0x0
 RM:strip_seg = 0x0
 RM:copy_seg = 0x0

```
show platform software fed switch ip multicast
```

```
=====
<output truncated>
```




PART **V**

IPv6

- [IPv6](#) , on page 267



IPv6

- [ipv6 dhcp server vrf enable](#), on page 268
- [ipv6 flow monitor](#) , on page 269
- [show ipv6 dhcp binding](#), on page 270

ipv6 dhcp server vrf enable

To enable the DHCP for IPv6 server VRF-aware feature, use the **ipv6 dhcp server vrf enable** command in global configuration mode. To disable the feature, use the **no** form of this command.

```
ipv6 dhcp server vrf enable
no ipv6 dhcp server vrf enable
```

Syntax Description This command has no arguments or keywords.

Command Default The DHCPv6 server VRF-aware feature is not enabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines The **ipv6 dhcp server option vpn** command allows the DHCPv6 server VRF-aware feature to be enabled globally on a device.

Examples The following example enables the DHCPv6 server VRF-aware feature globally on a device:

```
Device(config)# ipv6 dhcp server option vpn
```

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.

Command History

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

Usage Guidelines

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

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

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode.

show ipv6 dhcp binding [*ipv6-address*] [**vrf** *vrf-name*]

Syntax Description

<i>ipv6-address</i>	(Optional) The address of a DHCP for IPv6 client.
vrf <i>vrf-name</i>	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

The **show ipv6 dhcp binding** command displays all automatic client bindings from the DHCP for IPv6 server binding table if the *ipv6-address* argument is not specified. When the *ipv6-address* argument is specified, only the binding for the specified client is displayed.

If the **vrf** *vrf-name* keyword and argument combination is specified, all bindings that belong to the specified VRF are displayed.



Note

The **ipv6 dhcp server vrf enable** command must be enabled for the configured VRF to work. If the command is not configured, the output of the **show ipv6 dhcp binding** command will not display the configured VRF; it will only display the default VRF details.

Examples

The following sample output displays all automatic client bindings from the DHCP for IPv6 server binding table:

```
Device# show ipv6 dhcp binding

Client: FE80::A8BB:CCFF:FE00:300
DUID: 00030001AABBCC000300
Username : client_1
Interface: Virtual-Access2.1
IA PD: IA ID 0x000C0001, T1 75, T2 135
      Prefix: 2001:380:E00::/64
           preferred lifetime 150, valid lifetime 300
           expires at Dec 06 2007 12:57 PM (262 seconds)
Client: FE80::A8BB:CCFF:FE00:300 (Virtual-Access2.2)
DUID: 00030001AABBCC000300
IA PD: IA ID 0x000D0001, T1 75, T2 135
```

```
Prefix: 2001:0DB8:E00:1::/64
preferred lifetime 150, valid lifetime 300
expires at Dec 06 2007 12:58 PM (288 seconds)
```

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

Table 16: show ipv6 dhcp binding Field Descriptions

Field	Description
Client	Address of a specified client.
DUID	DHCP unique identifier (DUID).
Virtual-Access2.1	First virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but a different identity association for prefix delegation (IAPD) on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.
Username : client_1	The username associated with the binding.
IA PD	Collection of prefixes assigned to a client.
IA ID	Identifier for this IAPD.
Prefix	Prefixes delegated to the indicated IAPD on the specified client.
preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime settings, in seconds, for the specified client.
Expires at	Date and time at which the valid lifetime expires.
Virtual-Access2.2	Second virtual client. When an IPv6 DHCP client requests two prefixes with the same DUID but different IAIDs on two different interfaces, these prefixes are considered to be for two different clients, and interface information is maintained for both.

When the DHCPv6 pool on the Cisco IOS DHCPv6 server is configured to obtain prefixes for delegation from an authentication, authorization, and accounting (AAA) server, it sends the PPP username from the incoming PPP session to the AAA server for obtaining the prefixes. The PPP username associated with the binding is displayed in output from the **show ipv6 dhcp binding** command. If there is no PPP username associated with the binding, this field value is displayed as "unassigned."

The following example shows that the PPP username associated with the binding is "client_1":

```
Device# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
DUID: 0003000100AA00BB00CC
Username : client_1
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 75, T2 135
Prefix: 2001:0DB8:1:3::/80
preferred lifetime 150, valid lifetime 300
expires at Aug 07 2008 05:19 AM (225 seconds)
```

The following example shows that the PPP username associated with the binding is unassigned:

```
Device# show ipv6 dhcp binding

Client: FE80::2AA:FF:FE8B:CC
DUID: 0003000100AA00BB00CC
Username : unassigned
Interface : Virtual-Access2
IA PD: IA ID 0x00130001, T1 150, T2 240
Prefix: 2001:0DB8:1:1::/80
       preferred lifetime 300, valid lifetime 300
       expires at Aug 11 2008 06:23 AM (233 seconds)
```

Related Commands

Command	Description
ipv6 dhcp server vrf enable	Enables the DHCPv6 server VRF-aware feature.
clear ipv6 dhcp binding	Deletes automatic client bindings from the DHCP for IPv6 binding table.



PART VI

Layer 2/3

- [Layer 2/3](#) , on page 275



Layer 2/3

- [channel-group](#), on page 277
- [channel-protocol](#), on page 280
- [clear lacp](#), on page 281
- [clear pagp](#), on page 282
- [clear spanning-tree counters](#), on page 283
- [clear spanning-tree detected-protocols](#), on page 284
- [debug etherchannel](#), on page 285
- [debug lacp](#), on page 286
- [debug pagp](#), on page 287
- [debug platform pm](#), on page 288
- [debug platform uddl](#), on page 290
- [debug spanning-tree](#) , on page 291
- [interface port-channel](#), on page 293
- [lacp max-bundle](#), on page 294
- [lacp port-priority](#), on page 295
- [lacp rate](#), on page 296
- [lacp system-priority](#), on page 297
- [pagp learn-method](#), on page 298
- [pagp port-priority](#), on page 300
- [port-channel](#), on page 301
- [port-channel auto](#), on page 302
- [port-channel load-balance](#), on page 303
- [port-channel load-balance extended](#), on page 305
- [port-channel min-links](#), on page 306
- [rep admin vlan](#), on page 307
- [rep block port](#), on page 308
- [rep lsl-age-timer](#), on page 310
- [rep lsl-retries](#), on page 311
- [rep preempt delay](#), on page 312
- [rep preempt segment](#), on page 313
- [rep segment](#), on page 314
- [rep stcn](#), on page 316
- [show etherchannel](#), on page 317

- [show interfaces rep detail](#), on page 320
- [show lacp](#), on page 321
- [show pagp](#), on page 325
- [show platform software fed etherchannel](#), on page 327
- [show platform pm](#), on page 328
- [show rep topology](#), on page 329
- [show udd](#), on page 331
- [switchport](#), on page 334
- [switchport access vlan](#), on page 336
- [switchport mode](#), on page 339
- [switchport nonegotiate](#), on page 341
- [switchport voice vlan](#), on page 342
- [udd](#), on page 345
- [udd port](#), on page 347
- [udd reset](#), on page 349

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 device is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.



Caution

Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same device or on different devices in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.



Caution Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

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

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

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

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

This example shows how to configure a cross-stack EtherChannel in a device stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

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

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

channel-protocol

To restrict the protocol used on a port to manage channeling, use the **channel-protocol** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
channel-protocol {lacp | pagp}
no channel-protocol
```

Syntax Description

lacp Configures an EtherChannel with the Link Aggregation Control Protocol (LACP).

pagp Configures an EtherChannel with the Port Aggregation Protocol (PAgP).

Command Default

No protocol is assigned to the EtherChannel.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

You cannot configure PAgP on cross-stack configurations.

This example shows how to specify LACP as the protocol that manages the EtherChannel:

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

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

clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the **clear lacp** command in privileged EXEC mode.

clear lacp [*channel-group-number*] **counters**

Syntax Description	<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:

```
Device# clear lacp counters
```

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

```
Device# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp *channel-group-number* counters** privileged EXEC command.

clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the **clear pagp** command in privileged EXEC mode.

clear pagp [*channel-group-number*] **counters**

Syntax Description	<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:

```
Device# clear pagp counters
```

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

```
Device# clear pagp 10 counters
```

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

clear spanning-tree counters

To clear the spanning-tree counters, use the **clear spanning-tree counters** command in privileged EXEC mode.

clear spanning-tree counters [**interface** *interface-id*]

Syntax Description	interface <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	<p>If the <i>interface-id</i> value is not specified, spanning-tree counters are cleared for all interfaces.</p> <p>This example shows how to clear spanning-tree counters for all interfaces:</p> <pre>Device# clear spanning-tree counters</pre>	

clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring devices on the interface, use the **clear spanning-tree detected-protocols** command in privileged EXEC mode.

clear spanning-tree detected-protocols [**interface** *interface-id*]

Syntax Description	interface <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 device running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration method that enables it to interoperate with legacy IEEE 802.1D devices. If a rapid-PVST+ or an MSTP device receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, the device sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) device can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

The device does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs because it cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

This example shows how to restart the protocol migration process on a port:

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

debug etherchannel

To enable debugging of EtherChannels, use the **debug etherchannel** command in privileged EXEC mode. To disable debugging, use the **no** form of the command.

```
debug etherchannel [{all | detail | error | event | idb}]
no debug etherchannel [{all | detail | error | event | idb}]
```

Syntax Description

all	(Optional) Displays all EtherChannel debug messages.
detail	(Optional) Displays detailed EtherChannel debug messages.
error	(Optional) Displays EtherChannel error debug messages.
event	(Optional) Displays EtherChannel event messages.
idb	(Optional) Displays PAgP interface descriptor block debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.



Note Although the **linecard** keyword is displayed in the command-line help, it is not supported.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display all EtherChannel debug messages:

```
Device# debug etherchannel all
```

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

```
Device# debug etherchannel event
```

debug lacp

To enable debugging of Link Aggregation Control Protocol (LACP) activity, use the **debug lacp** command in privileged EXEC mode. To disable LACP debugging, use the **no** form of this command.

```
debug lacp [{all | event | fsm | misc | packet}]
no debug lacp [{all | event | fsm | misc | packet}]
```

Syntax Description

all	(Optional) Displays all LACP debug messages.
event	(Optional) Displays LACP event debug messages.
fsm	(Optional) Displays messages about changes within the LACP finite state machine.
misc	(Optional) Displays miscellaneous LACP debug messages.
packet	(Optional) Displays the receiving and transmitting LACP control packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebg etherchannel** command is the same as the **no debug etherchannel** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display all LACP debug messages:

```
Device# debug LACP all
```

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

```
Device# debug LACP event
```

debug pagp

To enable debugging of Port Aggregation Protocol (PAgP) activity, use the **debug pagp** command in privileged EXEC mode. To disable PAgP debugging, use the **no** form of this command.

```
debug pagp [{all | dual-active | event | fsm | misc | packet}]
no debug pagp [{all | dual-active | event | fsm | misc | packet}]
```

Syntax Description	
all	(Optional) Displays all PAgP debug messages.
dual-active	(Optional) Displays dual-active detection messages.
event	(Optional) Displays PAgP event debug messages.
fsm	(Optional) Displays messages about changes within the PAgP finite state machine.
misc	(Optional) Displays miscellaneous PAgP debug messages.
packet	(Optional) Displays the receiving and transmitting PAgP control packets.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines The **undebug pagp** command is the same as the **no debug pagp** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session switch-number** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command switch-number LINE** command in privileged EXEC mode.

This example shows how to display all PAgP debug messages:

```
Device# debug pagp all
```

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

```
Device# debug pagp event
```

debug platform pm

To enable debugging of the platform-dependent port manager software module, use the **debug platform pm** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status | platform |
pm-spi | pm-vectors [detail] | ses | vlans}
no debug platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status | platform
| pm-spi | pm-vectors [detail] | ses | vlans}
```

Syntax Description

all	Displays all port manager debug messages.
counters	Displays counters for remote procedure call (RPC) debug messages.
errdisable	Displays error-disabled-related events debug messages.
fec	Displays forwarding equivalence class (FEC) platform-related events debug messages.
if-numbers	Displays interface-number translation event debug messages.
l2-control	Displays Layer 2 control infra debug messages.
link-status	Displays interface link-detection event debug messages.
platform	Displays port manager function event debug messages.
pm-spi	Displays port manager stateful packet inspection (SPI) event debug messages.
pm-vectors	Displays port manager vector-related event debug messages.
detail	(Optional) Displays vector-function details.
ses	Displays service expansion shelf (SES) related event debug messages.
vlans	Displays VLAN creation and deletion event debug messages.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebg platform pm** command is the same as the **no debug platform pm** command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the **session *switch-number*** command in privileged EXEC mode. Enter the **debug** command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the **remote command** *switch-number LINE* command in privileged EXEC mode.

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Device# debug platform pm vlans
```

debug platform 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 device shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms.
synchronization	Displays the spanning-tree synchronization event debug messages.
uplinkfast	Displays UplinkFast-event debug messages.

Command Default Debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines The **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:

```
Device# debug spanning-tree all
```

interface port-channel

To access or create a port channel, use the **interface port-channel** command in global configuration mode. Use the **no** form of this command to remove the port channel.

```
interface port-channel port-channel-number
no interface port-channel
```

Syntax Description

port-channel-number Channel group number. The range is 1 to 128.

Command Default

No port channel logical interfaces are defined.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface before assigning physical ports to a channel group. Instead, you can use the **channel-group** interface configuration command, which automatically creates the port-channel interface when the channel group obtains its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number*, or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Only one port channel in a channel group is allowed.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it on the physical port and not on the port channel interface.
- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

This example shows how to create a port channel interface with a port channel number of 5:

```
Device(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel channel-group-number detail** privileged EXEC command.

lACP max-bundle

To define the maximum number of active LACP ports allowed in a port channel, use the **lACP max-bundle** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
lACP max-bundle max_bundle_number
no lACP max-bundle
```

Syntax Description	<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 device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **lACP max-bundle** command must specify a number greater than the number specified by the **port-channel min-links** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a maximum of five active LACP ports in port channel 2:

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

lACP port-priority

To configure the port priority for the Link Aggregation Control Protocol (LACP), use the **lACP port-priority** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

lACP port-priority *priority*
no lACP port-priority

Syntax Description

priority Port priority for LACP. The range is 1 to 65535.

Command Default

The default is 32768.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **lACP port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.

In port-priority comparisons, a numerically lower value has a higher priority: When there are more than eight ports in an LACP channel group, the eight ports with the numerically lowest values (highest priority values) for LACP port priority are bundled into the channel group, and the lower-priority ports are put in hot-standby mode. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), then an internal value for the port number determines the priority.



Note

The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the **lACP system-priority** global configuration command for determining which device controls the link.

Use the **show lACP internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the configuration guide for this release.

This example shows how to configure the LACP port priority on a port:

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

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

lacp rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the **lacp rate** command in interface configuration mode. To return to the default settings, use the **no** form of this command

```
lacp rate {normal | fast}
no lacp rate
```

Syntax Description	normal Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.				
	fast Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.				
Command Default	The default ingress rate for control packets is 30 seconds after the link is bundled.				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.2.1</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.2.1	This command was introduced.
Release	Modification				
Cisco IOS XE Denali 16.2.1	This command was introduced.				
Usage Guidelines	<p>Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate configured on the interface. Using the lacp rate command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.</p> <p>This command is supported only on LACP-enabled interfaces.</p> <p>This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:</p> <pre>Device(config)# interface gigabitEthernet 0/0 Device(config-if)# lacp rate fast</pre>				

lACP system-priority

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the **lACP system-priority** command in global configuration mode on the device. To return to the default setting, use the **no** form of this command.

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

Syntax Description	<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 device in an LACP link controls port priorities.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have a higher priority. Therefore, the system with the numerically lower value (higher priority value) for LACP system priority becomes the controlling system. If both devices have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the device MAC address) determines which device is in control.

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

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to set the LACP system priority:

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

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

pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the **pagp learn-method** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

Syntax Description	<p>aggregation-port Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.</p> <p>physical-port Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.</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 device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Device(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port channel within the EtherChannel:

```
Device(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp *channel-group-number* internal** privileged EXEC command.

pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the **pagp port-priority** command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the **no** form of this command.

pagp port-priority *priority*
no pagp port-priority

Syntax Description	<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 device supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the device hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports, such as the Catalyst 1900 switch.

When the link partner to the device is a physical learner, we recommend that you configure the device as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command. We also recommend that you set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

This example shows how to set the port priority to 200:

```
Device(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp channel-group-number internal** privileged EXEC command.

port-channel

To convert the auto created EtherChannel into a manual channel and adding configuration on the EtherChannel, use the **port-channel** command in privileged EXEC mode.

port-channel { *channel-group-number* **persistent** | **persistent** }

Syntax Description	<i>channel-group-number</i>	Channel group number. The range is 1 to 128.
	persistent	Converts the auto created EtherChannel into a manual channel and allows you to add configuration on the EtherChannel.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.7.2E	This command was introduced.
Usage Guidelines	You can use the show etherchannel summary privileged EXEC command to display the EtherChannel information.	

Examples

This example shows how to convert the auto created EtherChannel into a manual channel:

```
Device# port-channel 1 persistent
```

port-channel auto

To enable the auto-LAG feature on a switch globally, use the **port-channel auto** command in global configuration mode. To disable the auto-LAG feature on the switch globally, use **no** form of this command.

port-channel auto
no port-channel auto

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the auto-LAG feature is disabled globally and is enabled on all port interfaces.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE 3.7.2E	This command was introduced.

Usage Guidelines

You can use the **show etherchannel auto** privileged EXEC command to verify if the EtherChannel was created automatically.

Examples

This example shows how to enable the auto-LAG feature on the switch:

```
Device(config)# port-channel auto
```

port-channel load-balance

To set the load-distribution method among the ports in the EtherChannel, use the **port-channel load-balance** command in global configuration mode. To reset the load-balancing mechanism to the default setting, use the **no** form of this command.

```
port-channel load-balance {dst-ip | dst-mac | dst-mixed-ip-port | dst-port | extended | src-dst-ip |
src-dst-mac | src-dst-mixed-ip-port | src-dst-port | src-ip | src-mac | src-mixed-ip-port | src-port}
no port-channel load-balance
```

Syntax Description

dst-ip	Specifies load distribution based on the destination host IP address.
dst-mac	Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-mixed-ip-port	Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.
dst-port	Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
extended	Sets extended load balance methods among the ports in the EtherChannel. See the port-channel load-balance extended command.
src-dst-ip	Specifies load distribution based on the source and destination host IP address.
src-dst-mac	Specifies load distribution based on the source and destination host MAC address.
src-dst-mixed-ip-port	Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.
src-dst-port	Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.
src-ip	Specifies load distribution based on the source host IP address.
src-mac	Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-mixed-ip-port	Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.
src-port	Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

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

Usage Guidelines You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

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

```
Device(config)# port-channel load-balance dst-mac
```


port-channel load-balance extended

To set combinations of load-distribution methods among the ports in the EtherChannel, use the **port-channel load-balance extended** command in global configuration mode. To reset the extended load-balancing mechanism to the default setting, use the **no** form of this command.

```
port-channel load-balance extended[{dst-ip | dst-mac | dst-port | ipv6-label | l3-proto | src-ip | src-mac | src-port}]
no port-channel load-balance extended
```

Syntax Description

dst-ip	(Optional) Specifies load distribution based on the destination host IP address.
dst-mac	(Optional) Specifies load distribution based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel.
dst-port	(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.
ipv6-label	(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.
l3-proto	(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.
src-ip	(Optional) Specifies load distribution based on the source host IP address.
src-mac	(Optional) Specifies load distribution based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port.
src-port	(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.

Command Default

The default is **src-mac**.

Command Modes

Global configuration

Command History

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

Usage Guidelines

For information about when to use these forwarding methods, see the *Layer 2/3 Configuration Guide (Catalyst 3850 Switches)* for this release.

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

Examples

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

```
Device(config)# port-channel load-balance extended dst-ip dst-mac src-ip
```

port-channel min-links

To define the minimum number of LACP ports that must be bundled in the link-up state and bundled in the EtherChannel in order that a port channel becomes active, use the **port-channel min-links** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
port-channel min-links min_links_number
no port-channel min-links
```

Syntax Description	<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 device on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other device (the noncontrolling end of the link) are ignored.

The **port-channel min-links** command must specify a number a less than the number specified by the **lACP max-bundle** command.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag in the output display).

This example shows how to specify a minimum of three active LACP ports before port channel 2 becomes active:

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

rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for REP to transmit hardware flood layer (HFL) messages, use the **rep admin vlan** command in global configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep admin vlan vlan-id
no rep admin vlan
```

Syntax Description	<i>vlan-id</i> The 48-bit static MAC address.				
Command Default	The default value of the administrative VLAN is VLAN 1.				
Command Modes	Global configuration (config)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.2.2</td> <td>This command was introduced</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.2.2	This command was introduced
Release	Modification				
Cisco IOS XE Denali 16.2.2	This command was introduced				

Usage Guidelines

The range of the REP administrative VLAN is from 2 to 4094.

If you do not configure an administrative VLAN, the default VLAN is VLAN 1. The default VLAN 1 is always configured. There can be only one administrative VLAN on a router and on a segment.

You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

```
Device(config)# rep admin vlan 100
```

rep block port

To configure a REP VLAN load balancing on the REP primary edge port, use the **rep block port** command in interface configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the **no** form of this command.

```
rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
no rep block port {id port-id | neighbor-offset | preferred}
```

Syntax Description

id <i>port-id</i>	Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value. You can display the port ID for an interface by entering the show interface interface-id rep detail command in privileged EXEC mode.
<i>neighbor-offset</i>	Identifies the VLAN blocking alternate port by entering the offset number of a neighbor. The range is from -256 to +256; a value of 0 is invalid.
preferred	Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.
vlan	Identifies the VLANs to be blocked.
<i>vlan-list</i>	VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094 or a range or sequence of VLANs (such as 1-3, 22, 41-44) to be blocked.
all	Blocks all the VLANs.

Command Default

The default behavior after you enter the **rep preempt segment** command in privileged EXEC (for manual preemption) is to block all VLANs at the primary edge port. This behavior remains until you configure the **rep block port** command.

If the primary edge port cannot determine which port is to be the alternate port, the default action is no preemption and no VLAN load balancing.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines

You must enter this command on the REP primary edge port.

When you select an alternate port by entering an offset number, this number identifies the downstream neighbor port of an edge port. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors. Do not enter an offset value of 1 because that is the offset number of the primary edge port itself.

If you have configured a preempt delay time by entering the **rep preempt delay seconds** command in interface configuration mode and a link failure and recovery occurs, VLAN load balancing begins after the configured preemption time period elapses without another link failure. The alternate port specified in the load-balancing

configuration blocks the configured VLANs and unblocks all other segment ports. If the primary edge port cannot determine the alternate port for VLAN balancing, the default action is no preemption.

Each port in a segment has a unique port ID. To determine the port ID of a port, enter the **show interfaces interface-id rep detail** command in privileged EXEC mode.

The following example shows how to configure REP VLAN load balancing.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

rep lsl-age-timer

To configure the REP link status layer (LSL) age-out timer value, use the **rep lsl-age-timer** command in interface configuration mode. To restore the default age-out timer value, use the **no** form of this command.

```
rep lsl-age-timer milliseconds
no rep lsl-age-timer milliseconds
```

Syntax Description	<i>milliseconds</i> REP LSL age-out timer value in milliseconds (ms). The range is from 120 ms to 10000 ms in multiples of 40 ms.	
Command Default	The default LSL age-out timer value is 5 ms.	
Command Modes	Interface configuration (config-if)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.2	This command was introduced
Usage Guidelines	<p>The rep lsl-age-timer command is used to configure the REP LSL age-out timer value. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.</p> <p>The following example shows how to configure REP LSL age-out timer value.</p> <pre>Device(config)# interface TenGigabitEthernet 4/1 Device(config-if)# rep segment 1 edge primary Device(config-if)# rep lsl-age-timer 2000</pre>	

rep lsl-retries

To configure the REP link status layer (LSL) number of retries, use the **rep lsl-retries** command in interface configuration mode. To restore the default number of retries, use the **no** form of this command.

```
rep lsl-retries number-of-retries
no rep lsl-retries number-of-retries
```

Syntax Description

number-of-retries Number of LSL retries. The range of retries is from 3 to 10.

Command Default

The default number of LSL retries is 5.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines

The **rep lsl-retries** command is used to configure the number of retries before the REP link is disabled. While configuring REP configurable timers, we recommend that you configure the REP LSL number of retries first and then configure the REP LSL age-out timer value.

The following example shows how to configure REP LSL retries.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 2 edge primary
```

rep preempt delay

To configure a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered, use the **rep preempt delay** command in interface configuration mode. To remove the configured delay, use the **no** form of this command.

rep preempt delay *seconds*
no rep preempt delay

Syntax Description	<i>seconds</i> Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.				
Command Default	REP preemption delay is not set. The default is manual preemption without delay.				
Command Modes	Interface configuration (config-if)				
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Denali 16.2.2</td> <td>This command was introduced</td> </tr> </tbody> </table>	Release	Modification	Cisco IOS XE Denali 16.2.2	This command was introduced
Release	Modification				
Cisco IOS XE Denali 16.2.2	This command was introduced				

Usage Guidelines

You must enter this command on the REP primary edge port.

You must enter this command and configure a preempt time delay if you want VLAN load balancing to automatically trigger after a link failure and recovery.

If VLAN load balancing is configured, after a segment port failure and recovery, the REP primary edge port starts a delay timer before VLAN load balancing occurs. Note that the timer restarts after each link failure. When the timer expires, the REP primary edge alerts the alternate port to perform VLAN load balancing (configured by using the **rep block port** interface configuration command) and prepares the segment for the new topology. The configured VLAN list is blocked at the alternate port, and all other VLANs are blocked at the primary edge port.

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

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```


rep preempt segment

To manually start REP VLAN load balancing on a segment, use the **rep preempt segment** command in privileged EXEC mode.

```
rep preempt segment segment-id
```

Syntax Description	<i>segment-id</i> ID of the REP segment. The range is from 1 to 1024.	
Command Default	Manual preemption is the default behavior.	
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines

Enter this command on the segment, which has the primary edge port on the router.

Ensure that all the other segment configuration is completed before setting preemption for VLAN load balancing. When you enter the **rep preempt segment** *segment-id* command, a confirmation message appears before the command is executed because preemption for VLAN load balancing can disrupt the network.

If you do not enter the **rep preempt delay** *seconds* command in interface configuration mode on the primary edge port to configure a preemption time delay, the default configuration is to manually trigger VLAN load balancing on the segment. Use the **show rep topology** privileged EXEC command to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering this command results in the default behavior—the primary edge port blocks all VLANs.

You configure VLAN load balancing by entering the **rep block port** command in interface configuration mode on the REP primary edge port before you manually start preemption.

The following example shows how to manually trigger REP preemption on segment 100.

```
Device# rep preempt segment 100
```

rep segment

To enable REP on the interface and to assign a segment ID to the interface, use the **rep segment** command in interface configuration mode. To disable REP on the interface, use the **no** form of this command.

```
rep segment segment-id [edge [no-neighbor] [primary]] [preferred]
no rep segment
```

Syntax Description

<i>segment-id</i>	Segment for which REP is enabled. Assign a segment ID to the interface. The range is from 1 to 1024.
edge	(Optional) Configures the port as an edge port. Each segment has only two edge ports.
no-neighbor	(Optional) Specifies the segment edge as one with no external REP neighbor.
primary	(Optional) Specifies that the port is the primary edge port where you can configure VLAN load balancing. A segment has only one primary edge port.
preferred	(Optional) Specifies that the port is the preferred alternate port or the preferred port for VLAN load balancing.
Note	Configuring a port as preferred does not guarantee that it becomes the alternate port; it merely gives it a slight edge among equal contenders. The alternate port is usually a previously failed port.

Command Default

REP is disabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines

REP ports must be a Layer 2 IEEE 802.1Q port or 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port.

If REP is enabled on two ports on a router, both ports must be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a router is configured in a segment, the port should be an edge port.
- If two ports on a router belong to the same segment, both ports must be regular segment ports.
- If two ports on a router belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.

REP interfaces come up in a blocked state and remain in a blocked state until notified that it is safe to unblock. Be aware of this to avoid sudden connection losses.

When REP is enabled on an interface, the default is for the port to be a regular segment port.

The following example shows how to enable REP on a regular (nonedge) segment port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100
```

The following example shows how to enable REP on a port and identify the port as the REP primary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge primary
```

The following example shows how to enable REP on a port and identify the port as the REP secondary edge port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 100 edge
```

The following example shows how to enable REP as an edge no-neighbor port.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```

rep stcn

To configure a REP edge port to send segment topology change notifications (STCNs) to another interface or to other segments, use the **rep stcn** command in interface configuration mode. To disable the sending of STCNs to the interface or to the segment, use the **no** form of this command.

```
rep stcn {interface interface-id | segment segment-id-list}
no rep stcn {interface | segment}
```

Syntax Description

interface *interface-id* Specifies a physical interface or port channel to receive STCNs.

segment *segment-id-list* Specifies one REP segment or a list of segments to receive STCNs. The segment range is from 1 to 1024. You can also configure a sequence of segments (for example 3 to 5, 77, 100).

Command Default

Transmission of STCNs to other interfaces or segments is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines

Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50.

```
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```

show etherchannel

To display EtherChannel information for a channel, use the **show etherchannel** command in user EXEC mode.

```
show etherchannel [{channel-group-number} | {detail | port | port-channel | protocol | summary}]]
| [{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:

```
device# 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      Po1(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:

```

Device> show etherchannel 1 detail
Group state = L2
Ports: 2  Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:      LACP
                Ports in the group:
                -----
Port: Gi1/0/1
-----
Port state      = Up Mstr In-Bndl
Channel group = 1      Mode = Active      Gcchange = -
Port-channel   =      PolGC = -          Pseudo port-channel = Po1
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: Po1  (Primary Aggregator)

Age of the Port-channel = 01d:20h:20m:26s
Logical slot/port = 10/1      Number of ports = 2
HotStandBy port   = null
Port state        = Port-channel Ag-Inuse
Protocol          = LACP

Ports in the Port-channel:

Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----
0      00    Gi1/0/1   Active        0
0      00    Gi1/0/2   Active        0

Time since last port bundled: 01d:20h:24m:44s  Gi1/0/2

```

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

```

Device> show etherchannel 1 summary
Flags: D - down P - in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3 S - Layer2
      u - unsuitable for bundling
      U - in use f - failed to allocate aggregator
      d - default port

```

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

Group	Port-channel	Protocol	Ports
1	Po1 (SU)	LACP	Gi1/0/1 (P) Gi1/0/2 (P)

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

```
Device> show etherchannel 1 port-channel
Port-channels in the group:
-----
Port-channel: Po1 (Primary Aggregator)
-----
Age of the Port-channel = 01d:20h:24m:50s
Logical slot/port = 10/1 Number of ports = 2
Logical slot/port = 10/1 Number of ports = 2
Port state = Port-channel Ag-Inuse
Protocol = LACP

Ports in the Port-channel:

Index  Load  Port      EC state          No of bits
-----+-----+-----+-----+-----
  0     00   Gi1/0/1  Active            0
  0     00   Gi1/0/2  Active            0

Time since last port bundled: 01d:20h:24m:44s Gi1/0/2
```

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

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

show interfaces rep detail

To display detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

show interfaces [*interface-id*] **rep detail**

Syntax Description	
	<i>interface-id</i> (Optional) Physical interface used to display the port ID.

Command Modes	
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.2.2	This command was introduced

Usage Guidelines Enter this command on a segment edge port to send STCNs to one or more segments or to an interface. You can verify your settings by entering the **show interfaces rep detail** privileged EXEC command.

The following example shows how to display the REP configuration and status for a specified interface.

```
Device# show interfaces TenGigabitEthernet4/1 rep detail

TenGigabitEthernet4/1 REP enabled
Segment-id: 3 (Primary Edge)
PortID: 03010015FA66FF80
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 02040015FA66FF804050
Port Role: Open
Blocked VLAN: <empty>
Admin-vlan: 1
Preempt Delay Timer: disabled
Configured Load-balancing Block Port: none
Configured Load-balancing Block VLAN: none
STCN Propagate to: none
LSL PDU rx: 999, tx: 652
HFL PDU rx: 0, tx: 0
BPA TLV rx: 500, tx: 4
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 6, tx: 5
EPA-COMMAND TLV rx: 0, tx: 0
EPA-INFO TLV rx: 135, tx: 136
```


show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in user EXEC mode.

```
show lacp [channel-group-number] {counters | internal | neighbor | sys-id}
```

Syntax Description	
<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 device MAC address.

Command Default None

Command Modes User EXEC

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

Usage Guidelines You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* to specify a channel group for all keywords except **sys-id**.

This is an example of output from the **show lacp counters** user EXEC command. The table that follows describes the fields in the display.

```
Device> show lacp counters
          LACPDUs      Marker      Marker Response      LACPDUs
Port      Sent  Recv      Sent  Recv      Sent  Recv      Pkts  Err
-----
Channel group:1
Gi2/0/1   19   10         0    0         0    0         0
Gi2/0/2   14    6         0    0         0    0         0
```

Table 17: show lacp counters Field Descriptions

Field	Description
LACPDUs 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:

```
Device> show lacp 1 internal
Flags: S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode           P - Device is in Passive mode

Channel group 1

Port      Flags  State  LACP port  Admin  Oper  Port  Port
Port      Flags  State  Priority   Key    Key   Number State
Gi2/0/1   SA     bndl   32768     0x3    0x3   0x4   0x3D
Gi2/0/2   SA     bndl   32768     0x3    0x3   0x5   0x3D
```

The following table describes the fields in the display:

Table 18: 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:

```

Device> show lacp neighbor
Flags: S - Device is sending Slow LACPDUs   F - Device is sending Fast LACPDUs
       A - Device is in Active mode          P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

Port          Partner                               Partner   Partner
Gi2/0/1      System ID                             Port Number Age      Flags
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:

```
Device> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

show pagp

To display Port Aggregation Protocol (PAgP) channel-group information, use the **show pagp** command in EXEC mode.

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor}
```

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

```
Device> show pagp 1 counters
          Information      Flush
Port      Sent   Recv   Sent   Recv
-----
Channel group: 1
  Gi1/0/1   45    42     0     0
  Gi1/0/2   45    41     0     0
```

This is an example of output from the **show pagp dual-active** command:

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

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

<output truncated>
```

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

```
Device> show pagp 1 internal
Flags: S - Device is sending Slow hello.   C - Device is in Consistent state.
      A - Device is in Auto mode.
Timers: H - Hello timer is running.       Q - Quit timer is running.
      S - Switching timer is running.     I - Interface timer is running.

Channel group 1

```

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:

```
Device> show pagp 1 neighbor

Flags: S - Device is sending Slow hello.   C - Device is in Consistent state.
      A - Device is in Auto mode.           P - Device learns on physical port.

Channel group 1 neighbors

```

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

show platform software fed etherchannel

To display platform-dependent EtherChannel information, use the **show platform software fed etherchannel** command in privileged EXEC mode.

```
show platform software fed etherchannel [switch switch-number] channel-group-number
{group-mask | load-balance mac src-mac dst-mac [ip src-ip dst-ip [port src-port dst-port]]}
```

Syntax Description	
switch <i>switch-number</i>	(Optional) Specifies the stack member.
<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.

Command Default None

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	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 rep topology

To display REP topology information for a segment or for all segments, including the primary and secondary edge ports in the segment, use the **show rep topology** command in privileged EXEC mode.

show rep topology [**segment** *segment-id*] [**archive**] [**detail**]

Syntax Description		
segment <i>segment-id</i>		(Optional) Specifies the segment for which to display REP topology information. The ID range is from 1 to 1024.
archive		(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.
detail		(Optional) Displays detailed REP topology information.
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.2.2	This command was introduced

The following is sample output from the show rep topology command.

```
Device# show rep topology

REP Segment 1
BridgeName      PortName      Edge Role
-----
10.64.106.63    Te5/4         Pri  Open
10.64.106.228  Te3/4         Open
10.64.106.228  Te3/3         Open
10.64.106.67   Te4/3         Open
10.64.106.67   Te4/4         Alt
10.64.106.63   Te4/4         Sec  Open

REP Segment 3
BridgeName      PortName      Edge Role
-----
10.64.106.63    Gi50/1        Pri  Open
SVT_3400_2      Gi0/3         Open
SVT_3400_2      Gi0/4         Open
10.64.106.68    Gi40/2        Open
10.64.106.68    Gi40/1        Open
10.64.106.63    Gi50/2        Sec  Alt
```

The following is sample output from the **show rep topology detail** command.

```
Device# show rep topology detail

REP Segment 1
```

```
10.64.106.63, Te5/4 (Primary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
  Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
  Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
  Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
  Neighbor Number: 6 / [-1]
```

show 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.

```
Device> show udld gigabitethernet2/0/1
Interface gi2/0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
Entry 1
Expiration time: 146
Device ID: 1
Current neighbor state: Bidirectional
Device name: Switch-A
Port ID: Gi2/0/1
Neighbor echo 1 device: Switch-B
Neighbor echo 1 port: Gi2/0/2
Message interval: 5
CDP Device name: Switch-A
```

Table 19: show udld Field Descriptions

Field	Description
Interface	The interface on the local device configured for UDLD.
Port enable administrative configuration setting	How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting.
Port enable operational state	Operational state that shows whether UDLD is actually running on this port.
Current bidirectional state	The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring.

Field	Description
Current operational state	The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase.
Message interval	How often advertisement messages are sent from the local device. Measured in seconds.
Time out interval	The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window.
Entry 1	Information from the first cache entry, which contains a copy of echo information received from the neighbor.
Expiration time	The amount of time in seconds remaining before this cache entry is aged out.
Device ID	The neighbor device identification.
Current neighbor state	The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear.
Device name	The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch).
Port ID	The neighbor port ID enabled for UDLD.
Neighbor echo 1 device	The device name of the neighbors' neighbor from which the echo originated.
Neighbor echo 1 port	The port number ID of the neighbor from which the echo originated.
Message interval	The rate, in seconds, at which the neighbor is sending advertisement messages.
CDP device name	The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch).

This is an example of output from the **show udld neighbors** command:

```
Device# show udld neighbors
Port      Device Name      Device ID  Port-ID  OperState
-----
Gi2/0/1   Switch-A         1         Gi2/0/1  Bidirectional
Gi3/0/1   Switch-A         2         Gi3/0/1  Bidirectional
```

switchport

To put an interface that is in Layer 3 mode into Layer 2 mode for Layer 2 configuration, use the **switchport** command in interface configuration mode. To put an interface in Layer 3 mode, use the **no** form of this command.

switchport
no switchport

Syntax Description This command has no arguments or keywords.

Command Default By default, all interfaces are in Layer 2 mode.

Command Modes Interface configuration

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

Usage Guidelines Use the **no switchport** command (without parameters) to set the interface to the routed-interface status and to erase all Layer 2 configurations. You must use this command before assigning an IP address to a routed port.



Note This command is not supported on devices running the LAN Base feature set.

Entering the **no switchport** command shuts the port down and then reenables it, which might generate messages on the device to which the port is connected.

When you put an interface that is in Layer 2 mode into Layer 3 mode (or the reverse), the previous configuration information related to the affected interface might be lost, and the interface is returned to its default configuration.



Note If an interface is configured as a Layer 3 interface, you must first enter the **switchport** command to configure the interface as a Layer 2 port. Then you can enter the **switchport access vlan** and **switchport mode** commands.

The **switchport** command is not used on platforms that do not support Cisco-routed ports. All physical ports on such platforms are assumed to be Layer 2-switched interfaces.

You can verify the port status of an interface by entering the **show running-config** privileged EXEC command.

Examples

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

```
Device(config-if)# no switchport
```

This example shows how to cause the port interface to cease operating as a Cisco-routed port and convert to a Layer 2 switched interface:

```
Device(config-if)# switchport
```

switchport access vlan

To configure a port as a static-access port, use the **switchport access vlan** command in interface configuration mode. To reset the access mode to the default VLAN mode for the device, use the **no** form of this command.

switchport access vlan {*vlan-id* | **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:

```
Device(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:

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

Part 2 - Checking the VLAN database

```
Device # 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

```

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

```

Part 4 - Verifying configuration

```

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

```

Part 5 - Verifying interface switchport

```

Device # 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

```

```
Switch#
```

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	dynamic auto	dynamic desirable	trunk
	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.	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.	Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.	Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two devices or between a device and a router.
Command Default	The default mode is dynamic auto .			
Command Modes	Interface configuration			
Command History	Release	Modification		
	Cisco IOS XE 3.2SE	This command was introduced.		
Usage Guidelines	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>When you enter dynamic desirable mode, the interface becomes a trunk interface if the neighboring interface is set to trunk, desirable, or auto mode.</p>			

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:

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

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

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

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

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

switchport nonegotiate

To specify that Dynamic Trunking Protocol (DTP) negotiation packets are not sent on the Layer 2 interface, use the **switchport nonegotiate** command in interface configuration mode. Use the **no** form of this command to return to the default setting.

switchport nonegotiate
no switchport nonegotiate

Syntax Description

This command has no arguments or keywords.

Command Default

The default is to use DTP negotiation to learn the trunking status.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The **no switchport nonegotiate** command removes nonegotiate status.

This command is valid only when the interface switchport mode is access or trunk (configured by using the **switchport mode access** or the **switchport mode trunk** interface configuration command). This command returns an error if you attempt to execute it in dynamic (auto or desirable) mode.

Internetworking devices that do not support DTP might forward DTP frames improperly and cause misconfigurations. To avoid this problem, turn off DTP by using the **switchport nonegotiate** command to configure the interfaces connected to devices that do not support DTP to not forward DTP frames.

When you enter the **switchport nonegotiate** command, DTP negotiation packets are not sent on the interface. The device does or does not trunk according to the **mode** parameter: **access** or **trunk**.

- If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.
- To enable trunking on a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate** interface configuration commands to cause the interface to become a trunk but to not generate DTP frames.

This example shows how to cause a port to refrain from negotiating trunking mode and to act as a trunk or access port (depending on the mode set):

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

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

switchport voice vlan

To configure voice VLAN on the port, use the **switchport voice vlan** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

switchport voice vlan {*vlan-id* | **dot1p** | **none** | **untagged** | **name** *vlan_name*}
no switchport voice vlan

Syntax Description		
<i>vlan-id</i>		The VLAN to be used for voice traffic. The range is 1 to 4094. By default, the IP phone forwards the voice traffic with an IEEE 802.1Q priority of 5.
dot1p		Configures the telephone to use IEEE 802.1p priority tagging and uses VLAN 0 (the native VLAN). By default, the Cisco IP phone forwards the voice traffic with an IEEE 802.1p priority of 5.
none		Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.
untagged		Configures the telephone to send untagged voice traffic. This is the default for the telephone.
name <i>vlan_name</i>	(Optional)	Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.

Command Default The default is not to automatically configure the telephone (**none**).
 The telephone default is not to tag frames.

Command Modes Interface configuration

Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE Denali 16.2.1	Option to specify a VLAN name for voice VLAN. The ' name ' keyword was added.

Usage Guidelines You should configure voice VLAN on Layer 2 access ports.

You must enable Cisco Discovery Protocol (CDP) on the switch port connected to the Cisco IP phone for the device to send configuration information to the phone. CDP is enabled by default globally and on the interface.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the interface by entering the **trust device cisco-phone** interface configuration command. If you use the auto QoS feature, these settings are automatically configured.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The device puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select **dot1p**, **none**, or **untagged**, the device puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

A voice-VLAN port cannot be a private-VLAN port.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode: You can also verify your configuration by entering the **show interfaces interface-id switchport** in privileged EXEC command and examining information in the Voice VLAN: row.

Part 1 - Making the entry in the VLAN database:

```
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
Device#
```

Part 2 - Checking the VLAN database:

```
Device# show vlan id 55
VLAN Name Status Ports
-----
55 test active
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
55 enet 100055 1500 - - - - - 0 0
Remote SPAN VLAN
-----
Disabled
Primary Secondary Type Ports
-----
```

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

```
Device# configure terminal
Device(config)# interface gigabitethernet3/1/1
Device(config-if)# switchport mode access
Device(config-if)# switchport voice vlan name test
Device(config-if)# end
Device#
```

Part 4 - Verifying configuration:

```
Device# show running-config
interface gigabitethernet3/1/1
Building configuration...
Current configuration : 113 bytes
!
interface GigabitEthernet3/1/1
```

```
switchport voice vlan 55
switchport mode access
Switch#
```

Part 5 - Also can be verified in interface switchport:

```
Device# 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: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 55 (test)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Device#
```


udld

To enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time, use the **udld** command in global configuration mode. To disable aggressive or normal mode UDLD on all fiber-optic ports, use the **no** form of the command.

```
udld {aggressive | enable | message time message-timer-interval}
no udld {aggressive | enable | message}
```

Syntax Description		
	aggressive	Enables UDLD in aggressive mode on all fiber-optic interfaces.
	enable	Enables UDLD in normal mode on all fiber-optic interfaces.
	message time <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 reenable UDLD globally.
- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to reenable UDLD on the specified interface.

- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Device(config)# udld enable
```

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

udld port

To enable UniDirectional Link Detection (UDLD) on an individual interface or to prevent a fiber-optic interface from being enabled by the **udld** global configuration command, use the **udld port** command in interface configuration mode. To return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port, use the **no** form of this command.

udld port [**aggressive**]
no udld port [**aggressive**]

Syntax Description

aggressive (Optional) Enables UDLD in aggressive mode on the specified interface.

Command Default

On fiber-optic interfaces, UDLD is disabled and fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another device.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command resets all interfaces shut down by UDLD.
- The **shutdown** and **no shutdown** interface configuration commands.
- The **no udld enable** global configuration command, followed by the **udld {aggressive | enable}** global configuration command reenables UDLD globally.
- The **no udld port** interface configuration command, followed by the **udld port** or **udld port aggressive** interface configuration command reenables UDLD on the specified interface.

- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on an port:

```
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

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

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

udld reset

To reset all interfaces disabled by UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree, Port Aggregation Protocol (PAgP), and Dynamic Trunking Protocol (DTP) still have their normal effects, if enabled), use the **udld reset** command in privileged EXEC mode.

udld reset

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

This example shows how to reset all interfaces disabled by UDLD:

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




PART **VII**

Multiprotocol Label Switching (MPLS)

- [MPLS](#), on page 353
- [Multicast VPN](#), on page 363



MPLS

- [mpls ip default-route](#), on page 354
- [mpls ip \(global configuration\)](#), on page 355
- [mpls ip \(interface configuration\)](#), on page 356
- [mpls label protocol \(global configuration\)](#), on page 357
- [mpls label protocol \(interface configuration\)](#), on page 358
- [mpls label range](#), on page 359
- [show mpls label range](#), on page 361

mpls ip default-route

To enable the distribution of labels associated with the IP default route, use the **mpls ip default-route** command in global configuration mode.

mpls ip default-route

Syntax Description This command has no arguments or keywords.

Command Default No distribution of labels for the IP default route.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Dynamic label switching (that is, distribution of labels based on routing protocols) must be enabled before you can use the **mpls ip default-route** command.

Examples The following example shows how to enable the distribution of labels associated with the IP default route:

```
Switch# configure terminal
Switch(config)# mpls ip
Switch(config)# mpls ip default-route
```

Related Commands	Command	Description
	mpls ip (global configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
	mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.

mpls ip (global configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 and IPv6 packets along normally routed paths for the platform, use the **mpls ip** command in global configuration mode. To disable this feature, use the **no** form of this command.

mpls ip
no mpls ip

Syntax Description This command has no arguments or keywords.

Command Default Label switching of IPv4 and IPv6 packets along normally routed paths is enabled for the platform.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines MPLS forwarding of IPv4 and IPv6 packets along normally routed paths (sometimes called dynamic label switching) is enabled by this command. For a given interface to perform dynamic label switching, this switching function must be enabled for the interface and for the platform.

The **no** form of this command stops dynamic label switching for all platform interfaces regardless of the interface configuration; it also stops distribution of labels for dynamic label switching. However, the **no** form of this command does not affect the sending of labeled packets through label switch path (LSP) tunnels.

Examples

The following example shows that dynamic label switching is disabled for the platform, and all label distribution is terminated for the platform:

```
Switch(config)# no mpls ip
```

Related Commands	Command	Description
	mpls ip (interface configuration)	Enables MPLS forwarding of IPv4 and IPv6 packets along normally routed paths for the associated interface.

mpls ip (interface configuration)

To enable Multiprotocol Label Switching (MPLS) forwarding of IPv4 and IPv6 packets along normally routed paths for a particular interface, use the **mpls ip** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

mpls ip
no mpls ip

Syntax Description This command has no arguments or keywords.

Command Default MPLS forwarding of IPv4 and IPv6 packets along normally routed paths for the interface is disabled.

Command Modes Interface configuration (config-if)

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines MPLS forwarding of IPv4 and IPv6 packets along normally routed paths is sometimes called dynamic label switching. If dynamic label switching has been enabled for the platform when this command is issued on an interface, label distribution for the interface begins with the periodic transmission of neighbor discovery Hello messages on the interface. When the outgoing label for a destination routed through the interface is known, packets for the destination are labeled with that outgoing label and forwarded through the interface.

The **no** form of this command causes packets routed out through the interface to be sent unlabeled; this form of the command also terminates label distribution for the interface. However, the no form of the command does not affect the sending of labeled packets through any link-state packet (LSP) tunnels that might use the interface.

Examples

The following example shows how to enable label switching on the specified Ethernet interface:

```
Switch(config)# configure terminal
Switch(config-if)# interface TenGigabitEthernet1/0/3
Switch(config-if)# mpls ip
```

The following example shows that label switching is enabled on the specified vlan interface (SVI) on a Cisco Catalyst switch:

```
Switch(config)# configure terminal
Switch(config-if)# interface vlan 1
Switch(config-if)# mpls ip
```

mpls label protocol (global configuration)

To specify the Label Distribution Protocol (LDP) for a platform, use the **mpls label protocol** command in global configuration mode. To restore the default LDP, use the **no** form of this command.

mpls label protocol ldp
no mpls label protocol ldp

Syntax Description

ldp	Specifies that LDP is the default label distribution protocol.
------------	--

Command Default

LDP is the default label distribution protocol.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

If neither the global **mpls label protocol ldp** command nor the interface **mpls label protocol ldp** command is used, all label distribution sessions use LDP.

Examples

The following command establishes LDP as the label distribution protocol for the platform:

```
Switch(config)# mpls label protocol ldp
```

mpls label protocol (interface configuration)

To specify the label distribution protocol for an interface, use the **mpls label protocol** command in interface configuration mode. To remove the label distribution protocol from the interface, use the **no** form of this command.

mpls label protocol ldp
no mpls label protocol ldp

Syntax Description

ldp	Specifies that the label distribution protocol (LDP) is to be used on the interface.
------------	--

Command Default

If no protocol is explicitly configured for an interface, the label distribution protocol that was configured for the platform is used. To set the platform label distribution protocol, use the global **mpls label protocol** command.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

To successfully establish a session for label distribution for a link connecting two label switch routers (LSRs), the link interfaces on the LSRs must be configured to use the same label distribution protocol. If there are multiple links connecting two LSRs, all of the link interfaces connecting the two LSRs must be configured to use the same protocol.

Examples

The following example shows how to establish LDP as the label distribution protocol for the interface:

```
Switch(config-if)# mpls label protocol ldp
```

mpls label range

To configure the range of local labels available for use with Multiprotocol Label Switching (MPLS) applications on packet interfaces, use the **mpls label range** command in global configuration mode. To revert to the platform defaults, use the **no** form of this command.

mpls label range *minimum-value maximum-value* [**static** *minimum-static-value maximum-static-value*]
no mpls label range

Syntax Description		
<i>minimum-value</i>		The value of the smallest label allowed in the label space. The default is 16.
<i>maximum-value</i>		The value of the largest label allowed in the label space. The default is platform-dependent.
static		(Optional) Reserves a block of local labels for static label assignments. If you omit the static keyword and the <i>minimum-static-value maximum-static-value</i> arguments, no labels are reserved for static assignment.
<i>minimum-static-value</i>		(Optional) The minimum value for static label assignments. There is no default value.
<i>maximum-static-value</i>		(Optional) The maximum value for static label assignments. There is no default value.

Command Default The platform's default values are used.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The labels 0 through 15 are reserved by the IETF (see RFC 3032, MPLS Label Stack Encoding, for details) and cannot be included in the range specified in the **mpls label range** command. If you enter a 0 in the command, you will get a message that indicates that the command is an unrecognized command.

The label range defined by the **mpls label range** command is used by all MPLS applications that allocate local labels (for dynamic label switching, MPLS traffic engineering, MPLS Virtual Private Networks (VPNs), and so on).

You can use label distribution protocols, such as Label Distribution Protocol (LDP), to reserve a generic range of labels from 16 through 1048575 for dynamic assignment.

You specify the optional **static** keyword, to reserve labels for static assignment. The MPLS Static Labels feature requires that you configure a range of labels for static assignment. You can configure static bindings only from the current static range. If the static range is not configured or is exhausted, then you cannot configure static bindings.

The range of label values is 16 to 4096. The maximum value defaults to 4096. You can split for static label space between say 16 to 100 and for dynamic label space between 101 to 4096.

The upper and lower minimum static label values are displayed in the help line. For example, if you configure the dynamic label with a minimum value of 16 and a maximum value of 100, the help lines display as follows:

```
Switch(config)# mpls label range 16 100 static ?
<100> Upper Minimum static label value
<16> Lower Minimum static label value
Reserved Label Range --> 0 to 15
Available Label Range --> 16 to 4096
Static Label Range --> 16 to 100
Dynamic Label Range --> 101 to 4096
```

In this example, you can configure a static range from 16 to 100.

If the lower minimum static label space is not available, the lower minimum is not displayed in the help line. For example:

```
Switch(config)# mpls label range 16 100 static ?
<16-100> static label value range
```

Examples

The following example shows how to configure the size of the local label space. In this example, the minimum static value is set to 200, and the maximum static value is set to 4000.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# mpls label range 200 4000
Switch(config)#
```

If you had specified a new range that overlaps the current range (for example, the new range of the minimum static value set to 16 and the maximum static value set to 1000), then the new range takes effect immediately.

The following example show how to configure a dynamic local label space with a minimum static value set to 100 and the maximum static value set to 1000 and a static label space with a minimum static value set to 16 and a maximum static value set to 99:

```
Switch(config)# mpls label range 100 1000 static 16 99
Switch(config)#
```

In the following output, the **show mpls label range** command, executed after a reload, shows that the configured range is now in effect:

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 100/1000
Range for static labels: Min/Max/Number: 16/99
```

The following example shows how to restore the label range to its default value:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no mpls label range
Switch(config)# end
```

Related Commands

Command	Description
show mpls label range	Displays the range of the MPLS local label space.

show mpls label range

To display the range of local labels available for use on packet interfaces, use the `show mpls label range` command in privileged EXEC mode.

show mpls label range

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

You can use the `mpls label range` command to configure a range for local labels that is different from the default range. The `show mpls label range` command displays both the label range currently in use and the label range that will be in use following the next switch reload.

Examples

In the following example, the use of the `show mpls label range` command is shown before and after the `mpls label range` command is used to configure a label range that does not overlap the starting label range:

```
Switch# show mpls label range
Downstream label pool: Min/Max label: 16/100
Switch# configure terminal
Switch(config)# mpls label range 101 4000
Switch(config)# exit
Switch# show mpls label range
Downstream label pool: Min/Max label: 101/4000
```

Related Commands

Command	Description
<code>mpls label range</code>	Configures a range of values for use as local labels.

show mpls label range



Multicast VPN

- [ip multicast-routing](#), on page 364
- [ip multicast mrinfo-filter](#), on page 365
- [mdt data](#), on page 366
- [mdt default](#), on page 368
- [mdt log-reuse](#), on page 370
- [show ip pim mdt bgp](#), on page 371
- [show ip pim mdt history](#), on page 372
- [show ip pim mdt receive](#), on page 373
- [show ip pim mdt send](#), on page 375

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

```
ip multicast-routing [vrf vrf-name]
no ip multicast-routing [vrf vrf-name]
```

Syntax Description

vrf vrf-name	(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRP) instance specified for the <i>vrf-name</i> argument.
---------------------	--

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config).

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.



Note

For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Switch(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Switch(config)#
ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Switch(config)#
no ip multicast-routing
```

The following example shows how to enable MDS in Cisco IOS XE Release 3.3S a specific VRF:

```
Switch(config)#
ip multicast-routing vrf vrf1
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip multicast mrimfo-filter

To filter multicast router information (mrimfo) request packets, use the **ip multicast mrimfo-filter** command in global configuration mode. To remove the filter on mrimfo requests, use the **no** form of this command.

```
ip multicast [vrf vrf-name] mrimfo-filter access-list
no ip multicast [vrf vrf-name] mrimfo-filter
```

Syntax Description	Parameter	Description
	vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
	<i>vrf-name</i>	(Optional) Name assigned to the VRF.
	<i>access-list</i>	IP standard numbered or named access list that determines which networks or hosts can query the local multicast device with the mrimfo command.

Command Default No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines The **ip multicast mrimfo-filter** command filters the mrimfo request packets from all of the sources denied by the specified access list. That is, if the access list denies a source, that source's mrimfo requests are filtered. mrimfo requests from any sources permitted by the ACL are allowed to proceed.

Examples

The following example shows how to filter mrimfo request packets from all hosts on network 192.168.1.1 while allowing requests from any other hosts:

```
ip multicast mrimfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

Related Commands	Command	Description
	mrimfo	Queries a multicast device about which neighboring multicast devices are peering with it.

mdt data

To specify a range of addresses to be used in the data multicast distribution tree (MDT) pool, use the **mdt data** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt data threshold *kb/s*
no mdt data threshold *kb/s*

Syntax Description

threshold <i>kb/s</i>	(Optional) Defines the bandwidth threshold value in kilobits per second (kb/s). The range is from 1 to 4294967.
------------------------------	---

Command Default

A data MDT pool is not configured.

Command Modes

VRF address family configuration (config-vrf-af)
 VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

A data MDT can include a maximum of 256 multicast groups per MVPN. Multicast groups used to create the data MDT are dynamically chosen from a pool of configured IP addresses.

Use the **mdt data** command to specify a range of addresses to be used in the data MDT pool. The threshold is specified in kb/s. Using the optional **list** keyword and *access-list* argument, you can define the (S, G) MVPN entries to be used in a data MDT pool, which would further limit the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the *access-list* argument.

You can access the **mdt data** command by using the **ip vrf** global configuration command. You can also access the **mdt data** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

The following example shows how to configure the range of group addresses for the MDT data pool. A threshold of 500 kb/s has been set, which means that if a multicast stream exceeds 1 kb/s, then a data MDT is created.

```
ip vrf vrf1
 rd 1000:1
  route-target export 10:27
  route-target import 10:27
  mdt default 236.1.1.1
  mdt data 228.0.0.0 0.0.0.127 threshold 500 list 101
!
.
.
!
ip pim ssm default
```

```
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
mdt default	Configures a default MDT group for a VPN VRF.

mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt default *group-address*
no mdt default *group-address*

Syntax Description

<i>group-address</i>	IP address of the default MDT group. This address serves as an identifier for the community in that provider edge (PE) devices configured with the same group address become members of the group, allowing them to receive packets sent by each other.
----------------------	---

Command Default

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

The default MDT group must be the same group configured on all PE devices that belong to the same VPN.

If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address will be the address used to source the Border Gateway Protocol (BGP) sessions.

A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the *group-address* argument.

You can access the **mdt default** command by using the **ip vrf** global configuration command. You can also access the **mdt default** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

In the following example, Protocol Independent Multicast (PIM) SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted.

```
ip vrf vrf1
 rd 1000:1
  mdt default 236.1.1.1
  mdt data 228.0.0.0 0.0.0.127 threshold 50
  mdt data threshold 50
  route-target export 1000:1
  route-target import 1000:1
!
```


Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.

mdt log-reuse

To enable the recording of data multicast distribution tree (MDT) reuse, use the **mdt log-reuse** command in VRF configuration or in VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt log-reuse
no mdt log-reuse

Syntax Description	This command has no arguments or keywords.
Command Default	The command is disabled.
Command Modes	VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused. You can access the **mdt log-reuse** command by using the **ip vrf** global configuration command. You can also access the **mdt log-reuse** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples The following example shows how to enable MDT log reuse:

```
mdt log-reuse
```

Related Commands	Command	Description
	mdt data	Configures the multicast group address range for data MDT groups.
	mdt default	Configures a default MDT group for a VPN VRF.

show ip pim mdt bgp

To show details about the Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group, use the `show ip pim mdt bgp` command in user EXEC or privileged EXEC mode.

show ip pim [vrf *vrf-name*] mdt bgp

Syntax Description

vrf <i>vrf-name</i>	(Optional) Displays information about the BGP advertisement of the RD for the MDT default group associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
----------------------------	---

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

Use this command to show detailed BGP advertisement of the RD for the MDT default group.

Examples

The following is sample output from the `show ip pim mdt bgp` command:

```
Device# show ip pim mdt bgp
MDT-default group 232.2.1.4
  rid:10.1.1.1 next_hop:10.1.1.1
```

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

Table 20: show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	The MDT default groups that have been advertised to this router.
rid:10.1.1.1	The BGP router ID of the advertising router.
next_hop:10.1.1.1	The BGP next hop address that was contained in the advertisement.

show ip pim mdt history

To display information about the history of data multicast distribution tree (MDT) groups that have been reused, use the **show ip pim mdt history** command in privileged EXEC mode.

show ip pim vrf *vrf-name* mdt history interval *minutes*

Syntax Description

vrf <i>vrf-name</i>	Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
interval <i>minutes</i>	Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

The output of the **show ip pim mdt history** command displays the history of reused MDT data groups for the interval specified with the **interval** keyword and *minutes* argument. The interval is from the past to the present, that is, from the time specified for the *minutes* argument to the time at which the command is issued.

Examples

The following is sample output from the **show ip pim mdt history** command:

```
Device# show ip pim vrf vrf1 mdt history interval 20
MDT-data send history for VRF - vrf1 for the past 20 minutes
MDT-data group      Number of reuse
  10.9.9.8           3
  10.9.9.9           2
```

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

Table 21: show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	The MDT data group for which information is being shown.
Number of reuse	The number of data MDTs that have been reused in this group.

show ip pim mdt receive

To display the data multicast distribution tree (MDT) group mappings received from other provider edge (PE) routers, use the **show ip pim mdt receive** command in privileged EXEC mode.

show ip pim vrf *vrf-name* mdt receive [detail]

Syntax Description	Field	Description
	vrf <i>vrf-name</i>	Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
	detail	(Optional) Provides a detailed description of the data MDT advertisements received.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then it will join this global address multicast group.

Examples

The following is sample output from the **show ip pim mdt receive** command using the **detail** keyword for further information:

```
Device# show ip pim vrf vpn8 mdt receive detail
Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

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

Table 22: show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of (S, G) pairs that are reusing this data MDT.
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.

Field	Description
flags:	<p>Information about the entry.</p> <ul style="list-style-type: none"> • A--candidate Multicast Source Discovery Protocol (MSDP) advertisement • B--bidirectional group • D--dense • C--connected • F--register flag • I--received source-specific host report • J--join shortest path source tree (SPT) • L--local • M--MSDP created entry • P--pruned • R--RP bit set • S--sparse • s--Source Specific Multicast (SSM) group • T--SPT bit set • X--proxy join timer running • U--URL Rendezvous Directory (URD) • Y--joined MDT data group • y--sending to MDT data group • Z--multicast tunnel

show ip pim mdt send

To display the data multicast distribution tree (MDT) groups in use, use the **show ip pim mdt send** command in privileged EXEC mode.

show ip pim vrf *vrf-name* mdt send

Syntax Description	vrf <i>vrf-name</i>	Displays the data MDT groups in use by the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <i>vrf-name</i> argument.
---------------------------	----------------------------	--

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines Use this command to show the data MDT groups in use by a specified MVRF.

Examples

The following is sample output from the **show ip pim mdt send** command:

```
Device# show ip pim vrf vpn8 mdt send
MDT-data send list for VRF:vpn8
  (source, group)                MDT-data group      ref_count
(10.100.8.10, 225.1.8.1)         232.2.8.0           1
(10.100.8.10, 225.1.8.2)         232.2.8.1           1
(10.100.8.10, 225.1.8.3)         232.2.8.2           1
(10.100.8.10, 225.1.8.4)         232.2.8.3           1
(10.100.8.10, 225.1.8.5)         232.2.8.4           1
(10.100.8.10, 225.1.8.6)         232.2.8.5           1
(10.100.8.10, 225.1.8.7)         232.2.8.6           1
(10.100.8.10, 225.1.8.8)         232.2.8.7           1
(10.100.8.10, 225.1.8.9)         232.2.8.8           1
(10.100.8.10, 225.1.8.10)        232.2.8.9           1
```

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

Table 23: show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of (S, G) pairs that are reusing this data MDT.

```
show ip pim mdt send
```




PART **VIII**

Network Management

- [Flexible NetFlow, on page 379](#)
- [Network Management , on page 451](#)



Flexible NetFlow

- [cache](#), on page 381
- [clear flow exporter](#), on page 384
- [clear flow monitor](#), on page 385
- [collect](#), on page 387
- [collect counter](#), on page 388
- [collect interface](#), on page 389
- [collect timestamp absolute](#), on page 390
- [collect transport tcp flags](#), on page 391
- [datalink flow monitor](#), on page 392
- [debug flow exporter](#), on page 393
- [debug flow monitor](#), on page 394
- [debug flow record](#), on page 395
- [debug sampler](#), on page 396
- [description](#), on page 397
- [destination](#), on page 398
- [dscp](#), on page 399
- [export-protocol netflow-v9](#), on page 400
- [exporter](#), on page 401
- [flow exporter](#), on page 402
- [flow monitor](#), on page 403
- [flow record](#), on page 404
- [ip flow monitor](#), on page 405
- [ipv6 flow monitor](#), on page 407
- [match datalink dot1q priority](#), on page 409
- [match datalink dot1q vlan](#), on page 410
- [match datalink ethertype](#), on page 411
- [match datalink mac](#), on page 412
- [match datalink vlan](#), on page 413
- [match flow cts](#), on page 414
- [match flow direction](#), on page 415
- [match interface](#), on page 416
- [match ipv4](#), on page 417
- [match ipv4 destination address](#), on page 418

- [match ipv4 source address, on page 419](#)
- [match ipv4 ttl, on page 420](#)
- [match ipv6, on page 421](#)
- [match ipv6 destination address, on page 422](#)
- [match ipv6 hop-limit, on page 423](#)
- [match ipv6 source address, on page 424](#)
- [match transport, on page 425](#)
- [match transport icmp ipv4, on page 426](#)
- [match transport icmp ipv6, on page 427](#)
- [mode random 1 out-of, on page 428](#)
- [option, on page 429](#)
- [record, on page 431](#)
- [sampler, on page 432](#)
- [show flow exporter, on page 433](#)
- [show flow interface, on page 435](#)
- [show flow monitor, on page 437](#)
- [show flow record, on page 442](#)
- [show sampler, on page 443](#)
- [source, on page 445](#)
- [template data timeout, on page 447](#)
- [transport, on page 448](#)
- [ttl, on page 449](#)

cache

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

```
cache {timeout {active | inactive | update} seconds | type {normal | permanent}}
no cache {timeout {active | inactive | update} | type}
```

Syntax Description		
timeout		Specifies the flow timeout.
active		Specifies the active flow timeout.
inactive		Specifies the inactive flow timeout.
update		Specifies the update timeout for a permanent flow cache.
<i>seconds</i>		The timeout value in seconds. The range is 30 to 604800 (7 days) for a normal flow cache. For a permanent flow cache the range is 1 to 604800 (7 days).
type		Specifies the type of the flow cache.
normal		Configures a normal cache type. The entries in the flow cache will be aged out according to the timeout active seconds and timeout inactive seconds settings. This is the default cache type.
permanent		Configures a permanent cache type. This cache type disables flow removal from the flow cache.

Command Default

The default flow monitor flow cache parameters are used.

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

- Cache type: normal
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 15 seconds
- Update timeout for a permanent flow cache: 1800 seconds

Command Modes

Flow monitor configuration

Command History

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

Usage Guidelines

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

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

The **cache timeout inactive** command also controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected. If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation. When you change the inactive flow timeout, the new timeout value takes effect immediately.

The **cache timeout update** command controls the periodic updates sent by the permanent type of cache. This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache. By default, this timer value is 1800 seconds (30 minutes).

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

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



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



Note A permanent cache uses update counters rather than delta counters. When a flow is exported, the counters represent the totals seen for the full lifetime of the flow and not the additional packets and bytes seen since the last export was sent.

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

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

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

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

The following example shows how to configure the permanent cache update timeout:

```
Device(config)# flow monitor FLOW-MONITOR-1
Device(config-flow-monitor)# cache timeout update 5000
```

The following example shows how to configure a normal cache:

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

clear flow exporter

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

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

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

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


clear flow monitor

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

```
clear flow monitor [name] monitor-name [{[cache] force-export | statistics}]
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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



Note The statistics for the cleared cache entries are maintained.

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

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



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

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

Examples

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

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

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

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

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

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

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

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

collect

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

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

Syntax Description

counter	Configures the number of bytes or packets in a flow as a non-key field for a flow record. For more information, see collect counter, on page 388 .
interface	Configures the input and output interface name as a non-key field for a flow record. For more information, see collect interface, on page 389 .
timestamp	Configures the absolute time of the first seen or last seen packet in a flow as a non-key field for a flow record. For more information, see collect timestamp absolute, on page 390 .
transport	Enables the collecting of transport TCP flags from a flow record. For more information, see collect transport tcp flags, on page 391 .

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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



Note

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

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

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

collect counter

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

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

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

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

Command Modes Flow record configuration

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

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

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

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

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

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

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

collect interface

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

```
collect interface {input | output}
no collect interface {input | output}
```

Syntax Description	<p>input Configures the input interface name as a non-key field and enables collecting the input interface from the flows.</p> <p>output Configures the output interface name as a non-key field and enables collecting the output interface from the flows.</p>				
Command Default	The input and output interface names are not configured as a non-key field.				
Command Modes	Flow record 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 Flexible NetFlow **collect** commands are used to configure non-key fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in non-key fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a non-key field does not create a new flow. In most cases, the values for non-key fields are taken from only the first packet in the flow.

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

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

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

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

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

collect timestamp absolute

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

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

Syntax Description

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

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

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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

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

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

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

collect transport tcp flags

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

collect transport tcp flags
no collect transport tcp flags

Syntax Description	This command has no arguments or keywords.				
Command Default	The transport layer fields are not configured as a non-key field.				
Command Modes	Flow record configuration				
Command History	<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 values of the transport layer fields are taken from all packets in the flow. You cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command. The following transport TCP flags are collected:

- **ack**—TCP acknowledgement flag
- **cwr**—TCP congestion window reduced flag
- **ece**—TCP ECN echo flag
- **fin**—TCP finish flag
- **psh**—TCP push flag
- **rst**—TCP reset flag
- **syn**—TCP synchronize flag
- **urg**—TCP urgent flag

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

The following example collects the TCP flags from a flow:

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

datalink flow monitor

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

```
datalink flow monitor monitor-name {input | output | sampler sampler-name}
no datalink flow monitor monitor-name {input | output | sampler sampler-name}
```

Syntax Description

<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	Enables the specified flow sampler for the flow monitor.
input	Monitors traffic that the switch receives on the interface.
output	Monitors traffic that the switch sends on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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



Note

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

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

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


debug flow exporter

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

```
debug flow exporter [[name] exporter-name] [{error | event | packets number}]
no debug flow exporter [[name] exporter-name] [{error | event | packets number}]
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

debug flow monitor

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

```
debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
no debug flow monitor [{error | [name] monitor-name [{cache [error] | error | packets packets}]}]
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

debug flow record

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

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

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

Command Modes Privileged EXEC

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

Examples

The following example enables debugging for the flow record:

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

debug sampler

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

```
debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling samples}]}]
no debug sampler [{detailed | error | [name] sampler-name [{detailed | error | sampling}]}]
```

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

description

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

description *description*
no description *description*

Syntax Description

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

Command Default

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

Command Modes

The following command modes are supported:

Flow exporter configuration

Flow monitor configuration

Flow record configuration

Command History

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

Usage Guidelines

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

The following example configures a description for a flow monitor:

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

destination

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

```
destination {hostnameip-address} vrf vrf-label
no destination {hostnameip-address} vrf vrf-label
```

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

Command Default An export destination is not configured.

Command Modes Flow exporter configuration

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

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

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

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

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

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

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

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

dscp

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

```
dscp dscp
no dscp dscp
```

Syntax Description	<i>dscp</i> DSCP to be used in the DSCP field in exported datagrams. The range is 0 to 63. The default is 0.				
Command Default	The differentiated services code point (DSCP) value is 0.				
Command Modes	Flow exporter configuration				
Command History	<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 return this command to its default setting, use the no dscp or default dscp flow exporter configuration command.				

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

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

export-protocol netflow-v9

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

export-protocol netflow-v9

Syntax Description This command has no arguments or keywords.

Command Default NetFlow Version 9 is enabled.

Command Modes Flow exporter configuration

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

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

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

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


exporter

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

```
exporter exporter-name
no exporter exporter-name
```

Syntax Description	<i>exporter-name</i> Name of a flow exporter that was previously configured.
---------------------------	--

Command Default	An exporter is not configured.
------------------------	--------------------------------

Command Modes	Flow monitor configuration
----------------------	----------------------------

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

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

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

Examples

The following example configures an exporter for a flow monitor:

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

flow exporter

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

flow exporter *exporter-name*
no flow exporter *exporter-name*

Syntax Description	<i>exporter-name</i> Name of the flow exporter that is being created or modified.
---------------------------	---

Command Default	Flexible NetFlow flow exporters are not present in the configuration.
------------------------	---

Command Modes	Global configuration
----------------------	----------------------

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

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

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

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

flow monitor

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

flow monitor *monitor-name*
no flow monitor *monitor-name*

Syntax Description	<i>monitor-name</i> Name of the flow monitor that is being created or modified.
---------------------------	---

Command Default	Flexible NetFlow flow monitors are not present in the configuration.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

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

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

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

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

flow record

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

flow record *record-name*
no flow record *record-name*

Syntax Description	<i>record-name</i> Name of the flow record that is being created or modified.
---------------------------	---

Command Default	A Flexible NetFlow flow record is not configured.
------------------------	---

Command Modes	Global configuration
----------------------	----------------------

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

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

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

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

ip flow monitor

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

```
ip flow monitor monitor-name [sampler sampler-name] {input | output}
no ip flow monitor monitor-name [sampler sampler-name] {input | output}
```

Syntax Description	
<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv4 traffic that the device receives on the interface.
output	Monitors IPv4 traffic that the device transmits on the interface.

Command Default A flow monitor is not enabled.

Command Modes Interface configuration

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

Usage Guidelines

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

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

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



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

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

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

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

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

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

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

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

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

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

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

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

ipv6 flow monitor

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

```
ipv6 flow monitor monitor-name [sampler sampler-name] {input | output}
no ipv6 flow monitor monitor-name [sampler sampler-name] {input | output}
```

Syntax Description	
<i>monitor-name</i>	Name of the flow monitor to apply to the interface.
sampler <i>sampler-name</i>	(Optional) Enables the specified flow sampler for the flow monitor.
input	Monitors IPv6 traffic that the device receives on the interface.
output	Monitors IPv6 traffic that the device transmits on the interface.

Command Default A flow monitor is not enabled.

Command Modes Interface configuration

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

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

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

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



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

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

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

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

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

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Device(config-if)# exit
Device(config)# interface gigabitethernet2/0/3
Device(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

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

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

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

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

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

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


match datalink dot1q priority

To configure the 802.1Q (dot1q) priority value as a key field for a flow record, use the **match datalink dot1q priority** command in flow record configuration mode. To disable the use of the priority as a key field for a flow record, use the **no** form of this command.

```
match datalink dot1q priority
no match datalink dot1q priority
```

Syntax Description	This command has no arguments or keywords.	
Command Default	The priority field is not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

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

The observation point of the **match datalink dot1q priority** command is the interface to which the flow monitor that contains the flow record with the command is applied.

The following example configures the 802.1Q priority as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink dot1q priority
```

match datalink dot1q vlan

To configure the 802.1Q (dot1q) VLAN value as a key field for a flow record, use the **match datalink dot1q vlan** command in flow record configuration mode. To disable the use of the 802.1Q VLAN value as a key field for a flow record, use the **no** form of this command.

```
match datalink dot1q vlan {input | output}
no match datalink dot1q vlan {input | output}
```

Syntax Description	input Configures the VLAN ID of traffic being received by the as a key field.
	output Configures the VLAN ID of traffic being transmitted by the as a key field.

Command Default	The 802.1Q VLAN ID is not configured as a key field.
------------------------	--

Command Modes	Flow record configuration
----------------------	---------------------------

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

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

The input and output keywords of the **match datalink dot1q vlan** command are used to specify the observation point that is used by the **match datalink dot1q vlan** command to create flows based on the unique 802.1q VLAN IDs in the network traffic.

The following example configures the 802.1Q VLAN ID of traffic being received by the as a key field for a flow record:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match datalink dot1q vlan input
```

match datalink ethertype

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

match datalink ethertype
no match datalink ethertype

Syntax Description This command has no arguments or keywords.

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

Command Modes Flow record configuration

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

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

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

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

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

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

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

match datalink mac

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

```
match datalink mac {destination address {input | output} | source address {input | output}}
no match datalink mac {destination address {input | output} | source address {input | output}}
```

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

Command Default MAC addresses are not configured as a key field.

Command Modes Flow record configuration

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

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

The **input** and **output** keywords are used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addressees in the network traffic.



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

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

The following example configures the use of the source MAC addresses of packets that are transmitted by the device as a key field for a flow record:

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

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

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

match datalink vlan

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

```
match datalink vlan {input | output}
no match datalink vlan {input | output}
```

Syntax Description	<p>input Configures the VLAN ID of traffic being received by the device as a key field.</p> <p>output Configures the VLAN ID of traffic being transmitted by the device as a key field.</p>				
Command Default	The VLAN ID is not configured as a key field.				
Command Modes	Flow record 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>A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.</p> <p>The input and output keywords of the match datalink vlan command are used to specify the observation point that is used by the match datalink vlan command to create flows based on the unique VLAN IDs in the network traffic.</p> <p>The following example configures the VLAN ID of traffic being received by the device as a key field for a flow record:</p> <pre>Device(config)# flow record FLOW-RECORD-1 Device(config-flow-record)# match datalink vlan input</pre>				

match flow cts

To configure CTS source group tag and destination group tag for a flow record, use the **match flow cts** command in flow record configuration mode. To disable the group tag as key field for a flow record, use the **no** form of this command.

match flow cts {source | destination} group-tag
no match flow cts {source | destination} group-tag

Syntax Description	cts destination group-tag	Configures the CTS destination field group as a key field.
	cts source group-tag	Configures the CTS source field group as a key field.
Command Default	The CTS destination or source field group, flow direction and the flow sampler ID are not configured as key fields.	
Command Modes	Flexible NetFlow flow record configuration (config-flow-record) Policy inline configuration (config-if-policy-inline)	
Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.
	Cisco IOS XE Denali 16.2.1	This command was reintroduced. This command was not supported in Cisco IOS XE Denali 16.1.x
Usage Guidelines	A flow record requires at least one key field before it can be used in a flow monitor. The key fields distinguish flows, with each flow having a unique set of values for the key fields. The key fields are defined using the match command.	

The following example configures the source group-tag as a key field:

```
Device(config)# flow record FLOW-RECORD-1
Device(config-flow-record)# match flow cts source group-tag
```

match flow direction

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

match flow direction
no match flow direction

Syntax Description This command has no arguments or keywords.

Command Default The flow direction is not configured as key fields.

Command Modes Flow record configuration

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

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

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

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

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

match interface

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

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

Syntax Description

input Configures the input interface as a key field.

output Configures the output interface as a key field.

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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

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

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

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


match ipv4

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

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

Syntax Description	
destination address	Configures the IPv4 destination address as a key field. For more information see match ipv4 destination address, on page 418 .
protocol	Configures the IPv4 protocol as a key field.
source address	Configures the IPv4 destination address as a key field. For more information see match ipv4 source address, on page 419 .
tos	Configures the IPv4 ToS as a key field.
ttl	Configures the IPv4 time-to-live (TTL) field as a key field for a flow record. For more information see match ipv4 ttl, on page 420 .
version	Configures the IP version from IPv4 header as a key field.

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

Command Modes Flow record configuration

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

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

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

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

match ipv4 destination address

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

match ipv4 destination address
no match ipv4 destination address

Syntax Description	This command has no arguments or keywords.
---------------------------	--

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

Command Modes	Flow record configuration
----------------------	---------------------------

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

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

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

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

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

match ipv4 source address

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

match ipv4 source address
no match ipv4 source address

Syntax Description	This command has no arguments or keywords.	
Command Default	The IPv4 source address is not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

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

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

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

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

match ipv4 ttl

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

match ipv4 ttl
no match ipv4 ttl

Syntax Description	This command has no arguments or keywords.	
Command Default	The IPv4 time-to-live (TTL) field is not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

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

The following example configures IPv4 TTL as a key field:

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

match ipv6

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

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

Syntax Description	Field	Description
	destination address	Configures the IPv4 destination address as a key field. For more information see match ipv6 destination address, on page 422 .
	hop-limit	Configures the IPv6 hop limit as a key field. For more information see match ipv6 hop-limit, on page 423 .
	protocol	Configures the IPv6 protocol as a key field.
	source address	Configures the IPv4 destination address as a key field. For more information see match ipv6 source address, on page 424 .
	traffic-class	Configures the IPv6 traffic class as a key field.
	version	Configures the IPv6 version from IPv6 header as a key field.

Command Default The IPv6 fields are not configured as a key field.

Command Modes Flow record configuration

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

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

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

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

match ipv6 destination address

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

match ipv6 destination address
no match ipv6 destination address

Syntax Description	This command has no arguments or keywords.	
Command Default	The IPv6 destination address is not configured as a key field.	
Command Modes	Flow record configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

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

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

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

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

match ipv6 hop-limit

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

match ipv6 hop-limit
no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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

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

match ipv6 source address

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

match ipv6 source address
no match ipv6 source address

Syntax Description This command has no arguments or keywords.

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

Command Modes Flow record configuration

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

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

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

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

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


match transport

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

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

Syntax Description	
destination-port	Configures the transport destination port as a key field.
icmp ipv4	Configures the ICMP IPv4 type field and the code field as key fields. For more information see, match transport icmp ipv4, on page 426 .
icmp ipv6	Configures the ICMP IPv6 type field and the code field as key fields. For more information see, match transport icmp ipv6, on page 427 .
igmp type	Configures time stamps based on the system uptime as a key field.
source-port	Configures the transport source port as a key field.

Command Default The transport fields are not configured as a key field.

Command Modes Flow record configuration

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

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

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

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

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

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

match transport icmp ipv4

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

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

Syntax Description

code Configures the IPv4 ICMP code as a key field.

type Configures the IPv4 ICMP type as a key field.

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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

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

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

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

match transport icmp ipv6

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

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

Syntax Description

code Configures the IPv6 ICMP code as a key field.

type Configures the IPv6 ICMP type as a key field.

Command Default

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

Command Modes

Flow record configuration

Command History

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

Usage Guidelines

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

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

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

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

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

mode random 1 out-of

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

mode random 1 out-of *window-size*
no mode

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

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

Command Modes Sampler configuration

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

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



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

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

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

option

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

option {**exporter-stats** | **interface-table** | **sampler-table**} [{**timeout** *seconds*}]
no option {**exporter-stats** | **interface-table** | **sampler-table**}

Syntax Description	exporter-stats	Configures the exporter statistics option for flow exporters.
	interface-table	Configures the interface table option for flow exporters.
	sampler-table	Configures the export sampler table option for flow exporters.
	timeout <i>seconds</i>	(Optional) Configures the option resend time in seconds for flow exporters. The range is 1 to 86400. The default is 600.
Command Default	The timeout is 600 seconds. All other optional data parameters are not configured.	
Command Modes	Flow exporter configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
	Cisco IOS XE 3.3SE	The application-table and usermac-table keywords were added.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

record

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

```
record record-name
no record
```

Syntax Description

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

Command Default

A flow record is not configured.

Command Modes

Flow monitor configuration

Command History

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

Usage Guidelines

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



Note

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

Examples

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

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

sampler

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

sampler *sampler-name*

no sampler *sampler-name*

Syntax Description	<i>sampler-name</i> Name of the flow sampler that is being created or modified.
---------------------------	---

Command Default	Flexible NetFlow flow samplers are not configured.
------------------------	--

Command Modes	Global configuration
----------------------	----------------------

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

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

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

Examples

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

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


show flow exporter

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

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

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

Command Default None

Command Modes Privileged EXEC

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

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

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

This table describes the significant fields shown in the display:

Table 24: show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Description	The description that you configured for the exporter, or the default description User defined.
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.
Output Features	Specifies whether the output-features command, which causes the output features to be run on Flexible NetFlow export packets, has been used or not.

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

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

show flow interface

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

show flow interface [*type number*]

Syntax Description

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

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Interface Ethernet1/0
  monitor:          FLOW-MONITOR-1
  direction:       Output
  traffic(ip):      on
Device# show flow interface gigabitethernet1/0/2
Interface Ethernet0/0
  monitor:          FLOW-MONITOR-1
  direction:       Input
  traffic(ip):      sampler SAMPLER-2#
```

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

Table 25: show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: <ul style="list-style-type: none"> • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.

Field	Description
traffic(ip)	<p data-bbox="467 296 1162 323">Indicates if the flow monitor is in normal mode or sampler mode.</p> <p data-bbox="467 342 724 369">The possible values are:</p> <ul data-bbox="505 388 1479 499" style="list-style-type: none"><li data-bbox="505 388 964 415">• on—The flow monitor is in normal mode.<li data-bbox="505 438 1479 499">• sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

show flow monitor

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

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

Syntax Description	broker	(Optional) Displays information about the state of the broker for the flow monitor
	detail	(Optional) Displays detailed information about the flow monitor broker.
	picture	(Optional) Displays a picture of the broker state.
	name	(Optional) Specifies the name of a flow monitor.
	<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.
	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:

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

Flow Monitor FLOW-MONITOR-1:
  Description:          Used for basic traffic analysis
```

```

Flow Record:      flow-record-1
Flow Exporter:   flow-exporter-1
                  flow-exporter-2

Cache:
  Type:           normal
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout: 1800 secs
  Update Timeout: 1800 secs

```

This table describes the significant fields shown in the display.

Table 26: 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 possible values are: <ul style="list-style-type: none"> • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
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.
Update Timeout	Current value for the update timeout in seconds.

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

```

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

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

DATALINK MAC SOURCE ADDRESS INPUT:        0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:    6400.F125.59E6
IPV6 SOURCE ADDRESS:                      2001:DB8::1
IPV6 DESTINATION ADDRESS:                 2001:DB8:1::1
TRNS SOURCE PORT:                         1111
TRNS DESTINATION PORT:                    2222
IP VERSION:                               6
IP PROTOCOL:                              6
IP TOS:                                    0x05
IP TTL:                                    11
tcp flags:                                 0x20
counter bytes long:                        132059538
counter packets long:                      1158417

```

This table describes the significant fields shown in the display.

Table 27: 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.

Field	Description
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

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

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

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

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

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

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

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

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



```
counter bytes long:          132059538
counter packets long:       1158417
```

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

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

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

show flow record

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

```
show flow record [{broker [{detail | picture}] | [name] record-name}]
```

Syntax Description	broker	(Optional) Displays information about the state of the broker for the Flexible NetFlow flow record.
	detail	(Optional) Displays detailed information about the flow record broker.
	picture	(Optional) Displays a picture of the broker state.
	name	(Optional) Specifies the name of a flow record.
	record-name	(Optional) Name of a user-defined flow record that was previously configured.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

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

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

show sampler

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

```
show sampler [{broker [{detail | picture}] | [name] sampler-name}]
```

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

Command Default None

Command Modes Privileged EXEC

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

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

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

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

This table describes the significant fields shown in the display.

Table 28: show sampler Field Descriptions

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

source

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

```
source interface-type interface-number
no source
```

Syntax Description	<table border="1"> <tr> <td data-bbox="386 569 592 604"><i>interface-type</i></td> <td data-bbox="597 569 1528 638">Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.</td> </tr> <tr> <td data-bbox="386 659 592 695"><i>interface-number</i></td> <td data-bbox="597 659 1528 728">Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.</td> </tr> </table>	<i>interface-type</i>	Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.	<i>interface-number</i>	Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.
<i>interface-type</i>	Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.				
<i>interface-number</i>	Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.				
Command Default	The IP address of the interface over which the Flexible NetFlow datagram is transmitted is used as the source IP address.				
Command Modes	Flow exporter configuration				
Command History	<table border="1"> <thead> <tr> <th data-bbox="386 926 609 961">Release</th> <th data-bbox="613 926 1528 961">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="386 982 609 1018">Cisco IOS XE 3.2SE</td> <td data-bbox="613 982 1528 1018">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 benefits of using a consistent IP source address for the datagrams that Flexible NetFlow sends include the following:</p> <ul style="list-style-type: none"> • The source IP address of the datagrams exported by Flexible NetFlow is used by the destination system to determine from which device the Flexible NetFlow data is arriving. If your network has two or more paths that can be used to send Flexible NetFlow datagrams from the device to the destination system and you do not specify the source interface from which the source IP address is to be obtained, the device uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive Flexible NetFlow datagrams from the same device, but with different source IP addresses. When the destination system receives Flexible NetFlow datagrams from the same device with different source IP addresses, the destination system treats the Flexible NetFlow datagrams as if they were being sent from different devices. To avoid having the destination system treat the Flexible NetFlow datagrams as if they were being sent from different devices, you must configure the destination system to aggregate the Flexible NetFlow datagrams it receives from all of the possible source IP addresses in the device into a single Flexible NetFlow flow. • If your device has multiple interfaces that can be used to transmit datagrams to the destination system, and you do not configure the source command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting Flexible NetFlow traffic. Creating and maintaining access lists for permitting Flexible NetFlow traffic from known sources and blocking it from unknown sources is easier when you limit the source IP address for Flexible NetFlow datagrams to a single IP address for each device that is exporting Flexible NetFlow traffic. 				

**Caution**

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

**Tip**

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

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

Examples

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

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

template data timeout

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

template data timeout *seconds*
no template data timeout *seconds*

Syntax Description	<i>seconds</i> Timeout value in seconds. The range is 1 to 86400. The default is 600.				
Command Default	The default template resend timeout for a flow exporter is 600 seconds.				
Command Modes	Flow exporter configuration				
Command History	<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

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

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

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

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

transport

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

```
transport udp udp-port
no transport udp udp-port
```

Syntax Description	udp <i>udp-port</i> Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.				
Command Default	Flow exporters use UDP on port 9995.				
Command Modes	Flow exporter configuration				
Command History	<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>To return this command to its default settings, use the no transport or default transport flow exporter configuration command.</p> <p>The following example configures UDP as the transport protocol and a UDP port number of 250:</p> <pre>Device(config)# flow exporter FLOW-EXPORTER-1 Device(config-flow-exporter)# transport udp 250</pre>				

ttl

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

```
ttl ttl
no ttl ttl
```

Syntax Description	<i>ttl</i> Time-to-live (TTL) value for exported datagrams. The range is 1 to 255. The default is 255.				
Command Default	Flow exporters use a TTL of 255.				
Command Modes	Flow exporter configuration				
Command History	<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>To return this command to its default settings, use the no ttl or default ttl flow exporter configuration command.</p> <p>The following example specifies a TTL of 15:</p> <pre>Device(config)# flow exporter FLOW-EXPORTER-1 Device(config-flow-exporter)# ttl 15</pre>				



Network Management

- [description \(ERSPAN\)](#), on page 453
- [destination \(ERSPAN\)](#), on page 454
- [erspan-id](#), on page 456
- [filter \(ERSPAN\)](#), on page 457
- [ip ttl \(ERSPAN\)](#), on page 459
- [ip wccp](#), on page 460
- [monitor capture \(interface/control plane\)](#), on page 462
- [monitor capture buffer](#), on page 466
- [monitor capture clear](#), on page 467
- [monitor capture export](#), on page 468
- [monitor capture file](#), on page 469
- [monitor capture limit](#), on page 471
- [monitor capture match](#), on page 472
- [monitor capture start](#), on page 473
- [monitor capture stop](#), on page 474
- [monitor session](#), on page 475
- [monitor session destination](#), on page 477
- [monitor session filter](#), on page 481
- [monitor session source](#), on page 483
- [monitor session type erspan-source](#), on page 485
- [origin](#), on page 486
- [show ip sla statistics](#), on page 488
- [show capability feature monitor](#), on page 490
- [show monitor](#), on page 491
- [show monitor capture](#), on page 493
- [show monitor session](#), on page 495
- [show platform software fed switch ip wccp](#), on page 497
- [show platform ip wccp](#), on page 499
- [show platform software swspan](#) , on page 500
- [snmp-server enable traps](#), on page 502
- [snmp-server enable traps bridge](#), on page 505
- [snmp-server enable traps bulkstat](#), on page 506
- [snmp-server enable traps call-home](#), on page 507

- `snmp-server enable traps cef`, on page 508
- `snmp-server enable traps cpu`, on page 509
- `snmp-server enable traps envmon`, on page 510
- `snmp-server enable traps errdisable`, on page 511
- `snmp-server enable traps flash`, on page 512
- `snmp-server enable traps isis`, on page 513
- `snmp-server enable traps license`, on page 514
- `snmp-server enable traps mac-notification`, on page 515
- `snmp-server enable traps ospf`, on page 516
- `snmp-server enable traps pim`, on page 517
- `snmp-server enable traps port-security`, on page 518
- `snmp-server enable traps power-ethernet`, on page 519
- `snmp-server enable traps snmp`, on page 520
- `snmp-server enable traps stackwise`, on page 521
- `snmp-server enable traps storm-control`, on page 523
- `snmp-server enable traps stpx`, on page 524
- `snmp-server enable traps transceiver`, on page 525
- `snmp-server enable traps vrfmib`, on page 526
- `snmp-server enable traps vstack`, on page 527
- `snmp-server engineID`, on page 528
- `snmp-server host`, on page 529
- `source (ERSPAN)`, on page 533
- `switchport mode access`, on page 534
- `switchport voice vlan`, on page 535

description (ERSPAN)

To describe an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **description** command in ERSPAN monitor source session configuration mode. To remove a description, use the **no** form of this command.

description *description*
no description

Syntax Description *description* Describes the properties for this session.

Command Default Description is not configured.

Command Modes ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The *description* argument can be up to 240 characters.

Examples The following example shows how to describe an ERSPAN source session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# description source1
```

Related Commands	Command	Description
	monitor session type erspan-source	Configures a local ERSPAN source session.

destination (ERSPAN)

To configure an Encapsulated Remote Switched Port Analyzer (ERSPAN) source session destination and specify destination properties, use the **destination** command in ERSPAN monitor source session configuration mode. To remove a destination session, use the **no** form of this command.

destination
no destination

Syntax Description	This command has no arguments or keywords.				
Command Default	A source session destination is not configured.				
Command Modes	ERSPAN monitor source session configuration mode (config-mon-erspan-src)				
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.				

Usage Guidelines ERSPAN traffic is GRE-encapsulated SPAN traffic that can only be processed by an ERSPAN destination session.

All ERSPAN source session (maximum 8) destination IP address need not be same. Enter the **ip address** command to configure the IP address for the ERSPAN destination sessions.

The ERSPAN source session destination IP address, which is configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to destination ports. Configure the same address in both the source and destination sessions with the **ip address** command.

Examples

The following example shows how to configure an ERSPAN source session destination and enter the ERSPAN monitor destination session configuration mode to specify the destination properties:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip address 10.1.1.1
Switch(config-mon-erspan-src-dst)#
```

The following sample output from the **show monitor session all** displays different IP addresses for source session destinations:

```
Switch# show monitor session all

Session 1
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session1
Destination IP Address : 10.1.1.1

Session 2
-----
Type : ERSPAN Source Session
```

```
Status : Admin Disabled
Description : session2
Destination IP Address : 192.0.2.1
```

```
Session 3
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session3
Destination IP Address : 198.51.100.1
```

```
Session 4
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session4
Destination IP Address : 203.0.113.1
```

```
Session 5
-----
Type : ERSPAN Source Session
Status : Admin Disabled
Description : session5
Destination IP Address : 209.165.200.225
```

Related Commands

Command	Description
erspan-id	Configures the ID used by the destination session to identify the ERSPAN traffic.
ip ttl	Configures TTL values for packets in the ERSPAN traffic.
monitor session type erspan-source	Configures a local ERSPAN source session.
origin	Configures an IP address used as the source of the ERSPAN traffic.

erspan-id

To configure the ID used by the destination session to identify the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **erspan-id** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

```
erspan-id erspan-ID
no erspan-id erspan-ID
```

Syntax Description	<i>erspan-id</i> ERSPAN ID used by the destination session. Valid values are from 1 to 1023.
---------------------------	--

Command Default	ERSPAN IDs for destination sessions are not configured.
------------------------	---

Command Modes	ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)
----------------------	---

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following example shows how to configure an ERSPAN ID for a destination session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# erspan-id 3
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

filter (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source VLAN filtering when the ERSPAN source is a trunk port, use the **filter** command in ERSPAN monitor source session configuration mode. To remove the configuration, use the **no** form of this command.

```
filter {ip access-group {standard-access-list extended-access-list acl-name} | ipv6 access-group acl-name
| mac access-group acl-name | vlan vlan-id [{,}] [{-}]
no filter {ip [{access-group | [{standard-access-list extended-access-list acl-name}]}] | ipv6
[access-group] | mac [access-group] | vlan vlan-id [{,}] [{-}]}
```

Syntax Description		
ip		Specifies the IP access control rules.
access-group		Specifies an access control group.
<i>standard-access-list</i>		Standard IP access list.
<i>extended-access-list</i>		Extended IP access list.
<i>acl-name</i>		Access list name.
ipv6		Specifies the IPv6 access control rules.
mac		Specifies the media access control (MAC) rules.
vlan <i>vlan-ID</i>		Specifies the ERSPAN source VLAN. Valid values are from 1 to 4094.
,		(Optional) Specifies another VLAN.
-		(Optional) Specifies a range of VLANs.

Command Default Source VLAN filtering is not configured.

Command Modes ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines You cannot include source VLANs and filter VLANs in the same session.

When you configure the **filter** command on a monitored trunk interface, only traffic on that set of specified VLANs is monitored.

Examples

The following example shows how to configure source VLAN filtering:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# filter vlan 3
```

Related Commands

Command	Description
monitor session type erspan-source	Configures a local ERSPAN source session.

ip ttl (ERSPAN)

To configure Time to Live (TTL) values for packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **ip ttl** command in ERSPAN monitor destination session configuration mode. To remove the TTL values, use the **no** form of this command,

```
ip ttl ttl-value
no ip ttl ttl-value
```

Syntax Description	<i>ttl-value</i> TTL value. Valid values are from 2 to 255.				
Command Default	TTL value is set as 255.				
Command Modes	ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)				
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.				

Examples

The following example shows how to configure TTL value for ERSPAN traffic:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# ip ttl 32
```

Related Commands	Command	Description
	destination	Configures an ERSPAN destination session and specifies destination properties.
	monitor session type erspan-source	Configures a local ERSPAN source session.

ip wccp

To enable the web cache service, and specify the service number that corresponds to a dynamic service that is defined by the application engine, use the **ip wccp** global configuration command on the device. Use the **no** form of this command to disable the service.

```
ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
no ip wccp {web-cache | service-number} [group-address groupaddress] [group-list access-list]
[redirect-list access-list] [password encryption-number password]
```

Syntax Description

web-cache	Specifies the web-cache service (WCCP Version 1 and Version 2).
<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 devices 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 device combines the password with the MD5 authentication value to create security for the connection between the device and the application engine. By default, no password is configured, and no authentication is performed.

Command Default

WCCP services are not enabled on the device.

Command Modes

Global configuration

Command History

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

Usage Guidelines

WCCP transparent caching bypasses Network Address Translation (NAT) when Cisco Express Forwarding switching is enabled. To work around this situation, configure WCCP transparent caching in the outgoing direction, enable Cisco Express Forwarding switching on the content engine interface, and specify the **ip wccp web-cache redirect out** command. Configure WCCP in the incoming direction on the inside interface by

specifying the **ip wccp redirect exclude in** command on the router interface facing the cache. This configuration prevents the redirection of any packets arriving on that interface.

You can also include a redirect list when configuring a service group. The specified redirect list will deny packets with a NAT (source) IP address and prevent redirection.

This command instructs a device to enable or disable support for the specified service number or the web-cache service name. A service number can be from 0 to 254. Once the service number or name is enabled, the router can participate in the establishment of a service group.

When the **no ip wccp** command is entered, the device terminates participation in the service group, deallocates space if none of the interfaces still have the service configured, and terminates the WCCP task if no other services are configured.

The keywords following the **web-cache** keyword and the *service-number* argument are optional and may be specified in any order, but only may be specified once.

Example

The following example configures a web cache, the interface connected to the application engine or the server, and the interface connected to the client:

```
Device(config)# ip wccp web-cache
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# no switchport
Device(config-if)# ip address 172.20.10.30 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# exit
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport
Device(config-if)#
*Dec 6 13:11:29.507: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to down

Device(config-if)# ip address 175.20.20.10 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# ip wccp web-cache group-listen
Device(config-if)# exit
```

monitor capture (interface/control plane)

To configure monitor capture points specifying an attachment point and the packet flow direction or add more attachment points to a capture point, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction or disable one of multiple attachment points on a capture point, use the **no** form of this command.

monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

no monitor capture {*capture-name*} {**interface** *interface-type interface-id* | **control-plane**} {**in** | **out** | **both**}

Syntax Description		
	<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:
	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.

Examples

To define a capture point using a physical interface as an attachment point:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```



Note The second command defines the core filter for the capture point. This is required for a functioning capture point unless you are using a CAPWAP tunneling attachment point in your capture point.

If you are using CAPWAP tunneling attachment points in your capture point, you cannot use core filters.

To define a capture point with multiple attachment points:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
Device# monitor capture mycap control-plane in
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
      monitor capture mycap control-plane in
```

To remove an attachment point from a capture point defined with multiple attachment points:

```
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
      monitor capture mycap control-plane in
Device# no monitor capture mycap control-plane
Device# show monitor capture mycap parameter
      monitor capture mycap interface GigabitEthernet1/0/1 in
```

To define a capture point with a CAPWAP attachment point:

```
Device# show capwap summary
```

```
CAPWAP Tunnels General Statistics:
      Number of Capwap Data Tunnels      = 1
      Number of Capwap Mobility Tunnels   = 0
      Number of Capwap Multicast Tunnels = 0
```

Name	APName	Type	PhyPort	If	Mode	McastIf
Ca0	AP442b.03a9.6715	data	Gi3/0/6		unicast	-

Name	SrcIP	SrcPort	DestIP	DstPort	DtlsEn	MTU	Xact
Ca0	10.10.14.32	5247	10.10.14.2	38514	No	1449	0

```
Device# monitor capture mycap interface capwap 0 both
Device# monitor capture mycap file location flash:mycap.pcap
Device# monitor capture mycap file buffer-size 1
Device# monitor capture mycap start
```

```
*Aug 20 11:02:21.983: %BUFCAP-6-ENABLE: Capture Point mycap enabled.on
```

```
Device# show monitor capture mycap parameter
```

monitor capture (interface/control plane)

```

monitor capture mycap interface capwap 0 in
monitor capture mycap interface capwap 0 out
monitor capture mycap file location flash:mycap.pcap buffer-size 1
Device#
Device# show monitor capture mycap

Status Information for Capture mycap
Target Type:
Interface: CAPWAP,
  Ingress:
0
  Egress:
0
Status : Active
Filter Details:
  Capture all packets
Buffer Details:
  Buffer Type: LINEAR (default)
File Details:
  Associated file name: flash:mycap.pcap
  Size of buffer(in MB): 1
Limit Details:
  Number of Packets to capture: 0 (no limit)
  Packet Capture duration: 0 (no limit)
  Packet Size to capture: 0 (no limit)
  Packets per second: 0 (no limit)
  Packet sampling rate: 0 (no sampling)
Device#
Device# show monitor capture file flash:mycap.pcap
 1  0.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 2  0.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 3  2.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 4  2.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 5  3.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 6  4.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 7  4.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 8  5.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
 9  5.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
10  6.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
11  8.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
12  9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
13  9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
14  9.225986 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
15  9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
16  9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
17  9.231998 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
18  9.236987 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
19 10.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
20 10.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
21 12.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....

```



```
22 12.239993 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
23 12.244997 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
24 12.244997 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
25 12.250994 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
26 12.256990 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
27 12.262987 10.10.14.2 -> 10.10.14.32 DTLSv1.0 Application Data
28 12.499974 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
29 12.802012 10.10.14.3 -> 10.10.14.255 NBNS Name query NB WPAD.<00>
30 13.000000 00:00:00:00:00:00 -> 3c:ce:73:39:c6:60 IEEE 802.11 Probe Request, SN=0, FN=0,
Flags=.....
```

monitor capture buffer

To configure the buffer for monitor capture (WireShark), use the **monitor capture buffer** command in privileged EXEC mode. To disable the monitor capture buffer or change the buffer back to a default linear buffer from a circular buffer, use the **no** form of this command.

```
monitor capture {capture-name} buffer {circular [size buffer-size ] | size buffer-size}
no monitor capture {capture-name} buffer [circular ]
```

Syntax Description	<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:

```
Device# monitor capture mycap buffer circular size 1
```

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

capture-name The name of the capture whose buffer is to be cleared.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Use the **monitor capture clear** command either during capture or after the capture has stopped either because one or more end conditions has been met, or you entered the **monitor capture stop** command. If you enter the **monitor capture clear** command after the capture has stopped, the **monitor capture export** command that is used to store the contents of the captured packets in a file will have no impact because the buffer has no captured packets.

If you have more than one capture that is storing packets in a buffer, clear the buffer before starting a new capture to avoid memory loss.

Example

To clear the buffer contents for capture mycap:

```
Device# monitor capture mycap clear
```

monitor capture export

To export a monitor capture (WireShark) to a file, use the **monitor capture export** command in privileged EXEC mode.

monitor capture {*capture-name*} **export** *file-location* : *file-name*

Syntax Description

capture-name The name of the capture to be exported.

file-location : *file-name* (Optional) Specifies the location and file name of the capture storage file.

Acceptable values for *file-location* :

- flash—On-board flash storage
- (usbflash0:)— USB drive

Command Default

The captured packets are not stored.

Command Modes

Privileged EXEC

Command History

Release

Cisco IOS XE 3.3SE

Modification

This command was introduced.

Usage Guidelines

Use the **monitor capture export** command only when the storage destination is a capture buffer. The file may be stored either remotely or locally. Use this command either during capture or after the packet capture has stopped. The packet capture is stopped when one or more end conditions have been met or you entered the **monitor capture stop** command.

When WireShark is used on switches in a stack, packet captures can be stored only on the devices specified for *file-location* above that are connected to the active switch. Example: flash1 is connected to the active switch. flash2 is connected to the secondary switch. Only flash1 can be used to store packet captures.



Note

Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.

Example

To export the capture buffer contents to mycap.pcap on a flash drive:

```
Device# monitor capture mycap export flash:mycap.pcap
```

monitor capture file

To configure monitor capture (WireShark) storage file attributes, use the **monitor capture file** command in privileged EXEC mode. To remove a storage file attribute, use the **no** form of this command.

```
monitor capture {capture-name} file{ [ buffer-size temp-buffer-size ] [ location file-location :  
file-name ] [ ring number-of-ring-files ] [ size total-size ] }  
no monitor capture {capture-name} file{ [ buffer-size ] [ location ] [ ring ] [ size ] }
```

Syntax Description		
<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:

```
Device# monitor capture mycap file location flash:mycap.pcap
```

monitor capture limit

To configure capture limits, use the **monitor capture limit** command in privileged EXEC mode. To remove the capture limits, use the **no** form of this command.

```
monitor capture {capture-name} limit { [duration seconds] [packet-length size] [packets num] }
no monitor capture {capture-name} limit [duration] [packet-length] [packets]
```

Syntax Description	
<i>capture-name</i>	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:

```
Device# monitor capture mycap limit duration 60 packet-len 400
```

monitor capture match



Note Do not use this command when capturing a CAPWAP tunnel. Also, when control plane and CAPWAP tunnels are mixed, this command will have no effect.

To define an explicit inline core filter for a monitor (Wireshark) capture, use the **monitor capture match** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

```
monitor capture {capture-name} match {any | mac mac-match-string | ipv4 {any | host | protocol}{any | host} | ipv6 {any | host | protocol}{any | host}}
no monitor capture {capture-name} match
```

Syntax Description

<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:

```
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```


monitor capture start

To start the capture of packet data at a traffic trace point into a buffer, use the **monitor capture start** command in privileged EXEC mode.

monitor capture { *capture-name* } **start**

Syntax Description

capture-name The name of the capture to be started.

Command Default

The buffer content is not cleared.

Command Modes

Privileged EXEC

Command History**Release****Modification**

Cisco IOS XE 3.3SE

This command was introduced.

Usage Guidelines

Use the **monitor capture clear** command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the **monitor capture stop** command.

Ensure that system resources such as CPU and memory are available before starting a capture.

Example

To start capturing buffer contents:

```
Device# monitor capture mycap start
```

monitor capture stop

To stop the capture of packet data at a traffic trace point, use the **monitor capture stop** command in privileged EXEC mode.

monitor capture {*capture-name*} **stop**

Syntax Description	<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:

```
Device# monitor capture mycap stop
```

monitor session

To create a new Ethernet Switched Port Analyzer (SPAN) or a Remote Switched Port Analyzer (RSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the **monitor session** global configuration command. To clear SPAN or RSPAN sessions, use the **no** form of this command.

```
monitor session session-number {destination | filter | source}
no monitor session {session-number [destination | filter | source] | all | local | range
session-range | remote}
```

Syntax Description		
<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.

```
Device(config)# monitor session 1 source interface Po13
Device(config)# monitor session 1 filter vlan 1281
Device(config)# monitor session 1 destination interface GigabitEthernet2/0/36 encapsulation
replicate
Device(config)# monitor session 1 destination interface GigabitEthernet3/0/36 encapsulation
replicate
```

The following is the output of a **show monitor session all** command after completing these setup instructions:

```
Device# show monitor session all

Session 1
-----
Type                : Local Session
Source Ports        :
  Both               : Po13
Destination Ports   : Gi2/0/36,Gi3/0/36
  Encapsulation     : Replicate
  Ingress            : Disabled
Filter VLANs        : 1281
...
```

monitor session destination

To start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) destination session, to enable ingress traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), and to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, use the **monitor session destination** global configuration command. To remove the SPAN or RSPAN session or to remove destination interfaces from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
no monitor session session-number destination {interface interface-id [, | -] [encapsulation
{replicate | dot1q} ] {ingress [dot1q | untagged] } | {remote} vlan vlan-id
```

Syntax Description	
<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:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Device(config)# no monitor session 2 destination interface gigabitethernet1/0/2
```

This example shows how to configure RSPAN source session 1 to monitor a source interface and to configure the destination RSPAN VLAN 900:

```
Device(config)# monitor session 1 source interface gigabitethernet1/0/1
Device(config)# monitor session 1 destination remote vlan 900
Device(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic:

```
Device(config)# monitor session 10 source remote vlan 900
Device(config)# monitor session 10 destination interface gigabitethernet1/0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation
dot1q ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Device(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress untagged
vlan 5
```


monitor session filter

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the **monitor session filter** global configuration command. To remove filters from the SPAN or RSPAN session, use the **no** form of this command.

```
monitor session session-number filter {vlan vlan-id [, | -] }
no monitor session session-number filter {vlan vlan-id [, | -] }
```

Syntax Description		
<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
```

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
```

monitor session type erspan-source

To configure a local Encapsulated Remote Switched Port Analyzer (ERSPAN) source session, use the **monitor session type erspan-source** command in global configuration mode. To remove the ERSPAN configuration, use the **no** form of this command.

```
monitor session span-session-number type erspan-source
no monitor session span-session-number type erspan-source
```

Syntax Description	<i>span-session-number</i>	Number of the local ERSPAN session. Valid values are from 1 to 66.
---------------------------	----------------------------	--

Command Default ERSPAN source session is not configured.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The *span-session-number* and the session type (configured by the *erspan-source* keyword) cannot be changed once configured. Use the **no** form of this command to remove the session and then re-create the session with a new session ID or a new session type.

The ERSPAN source session destination IP address, which must be configured on an interface on the destination switch, is the source of traffic that an ERSPAN destination session sends to the destination ports. You can configure the same address in both the source and destination sessions with the **ip address** command in ERSPAN monitor destination session configuration mode.

The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.

The maximum local ERSPAN source session limit is 8.

Examples

The following example shows how to configure an ERSPAN source session number:

```
Switch(config)# monitor session 55 type erspan-source
Switch(config-mon-erspan-src)#
```

Related Commands	Command	Description
	monitor session type	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.
	show capability feature monitor	Displays information about monitor features.
	show monitor session	Displays information about the ERSPAN, SPAN, and RSPAN sessions.

origin

To configure the IP address used as the source of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the **origin** command in ERSPAN monitor destination session configuration mode. To remove the configuration, use the **no** form of this command.

origin *ip-address*
no origin *ip-address*

Syntax Description

ip-address Specifies the ERSPAN source session destination IP address.

Command Default

Source IP address is not configured.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

ERSPAN source session on a switch can use different source IP addresses using the **origin** command.

Examples

The following example shows how to configure an IP address for an ERSPAN source session:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# destination
Switch(config-mon-erspan-src-dst)# origin ip-address 203.0.113.2
```

The following sample output from the **show monitor session all** command displays ERSPAN source sessions with different source IP addresses:

```
Session 3
-----
Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
Both : Gi1/0/13
Destination IP Address : 10.10.10.10
Origin IP Address : 10.10.10.10
```

```
Session 4
-----
Type : ERSPAN Source Session
Status : Admin Enabled
Destination IP Address : 192.0.2.1
Origin IP Address : 203.0.113.2
```

Related Commands

Command	Description
destination	Configures an ERSPAN destination session and specifies destination properties.
monitor session type erspan-source	Configures a local ERSPAN source session.

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:

```
Device# show ip sla statistics

Current Operational State
Entry Number: 3
Modification Time: *22:15:43.000 UTC Sun Feb 11 2001
Diagnostics Text:
Last Time this Entry was Reset: Never
Number of Octets in use by this Entry: 1332
Number of Operations Attempted: 2
Current Seconds Left in Life: 3511
Operational State of Entry: active
Latest Completion Time (milliseconds): 544
Latest Operation Start Time: *22:16:43.000 UTC Sun Feb 11 2001
Latest Oper Sense: ok
Latest Sense Description: 200 OK
```



```
Total RTT: 544  
DNS RTT: 12  
TCP Connection RTT: 28  
HTTP Transaction RTT: 504  
HTTP Message Size: 9707
```

show capability feature monitor

To display information about monitor features, use the **show capability feature monitor** command in privileged EXEC mode.

show capability feature monitor {erspan-destination | erspan-source}

Syntax Description	erspan-destination	erspan-source
	Displays information about the configured Encapsulated Remote Switched Port Analyzer (ERSPAN) source sessions.	Displays all the configured global built-in templates.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following is sample output from the **show capability feature monitor erspan-source** command:

```
Switch# show capability feature monitor erspan-source

ERSPAN Source Session Supported: true
No of Rx ERSPAN source session: 8
No of Tx ERSPAN source session: 8
ERSPAN Header Type supported: II
ACL filter Supported: true
Fragmentation Supported: true
Truncation Supported: false
Sequence number Supported: false
QOS Supported: true
```

The following is sample output from the **show capability feature monitor erspan-destination** command:

```
Switch# show capability feature monitor erspan-destination

ERSPAN Destination Session Supported: false
```

Related Commands

Command	Description
monitor session type erspan-source	Creates an ERSPAN source session number or enters the ERSPAN session configuration mode for the session.

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:

```
Device# show monitor
```

```

Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
Session 2
-----
Type : Remote Source Session
Source VLANs :
TX Only : 10
Both : 1-9
Dest RSPAN VLAN : 105

```

This is an example of output for the **show monitor** user EXEC command for local SPAN source session 1:

```

Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled

```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```

Device# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged

```

show monitor capture

To display monitor capture (WireShark) content, use the **show monitor capture file** command in privileged EXEC mode.

```
show monitor capture [capture-name [ buffer ] | file file-location : file-name ][ brief | detailed | display-filter display-filter-string ]
```

Syntax Description	
<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:

```
Device# show monitor capture mycap

Status Information for Capture mycap
  Target Type:
  Interface: CAPWAP,
  Ingress:
  0
  Egress:
  0
  Status : Active
  Filter Details:
    Capture all packets
  Buffer Details:
    Buffer Type: LINEAR (default)
  File Details:
    Associated file name: flash:mycap.pcap
    Size of buffer(in MB): 1
```

Limit Details:

```
Number of Packets to capture: 0 (no limit)
Packet Capture duration: 0 (no limit)
Packet Size to capture: 0 (no limit)
Packets per second: 0 (no limit)
Packet sampling rate: 0 (no sampling)
```

show monitor session

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the **show monitor session** command in EXEC mode.

```
show monitor session {session_number | all | erspan-source | local | range list | remote}
[detail]
```

Syntax Description

<i>session_number</i>	The session number identified with the SPAN or RSPAN session. The range is 1 to 68. However if this switch is stacked with Catalyst 2960-S switches, you are limited to a combined maximum of two local SPAN sessions and RSPAN source sessions, and the range is 1 to 66.
all	Displays all SPAN sessions.
erspan-source	Displays only source ERSPAN sessions.
local	Displays only local SPAN sessions.
range list	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	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 maximum local ERSPAN source session limit is 8.

Examples

The following is sample output from the **show monitor session** command for local SPAN source session 1:

```
Device# show monitor session 1
Session 1
-----
Type : Local Session
Source Ports :
RX Only : Gi4/0/1
Both : Gi4/0/2-3,Gi4/0/5-6
Destination Ports : Gi4/0/20
Encapsulation : Replicate
Ingress : Disabled
```

The following is sample output from the **show monitor session all** command when ingress traffic forwarding is enabled:

```
Device# show monitor session all
Session 1
-----
Type : Local Session
Source Ports :
Both : Gi4/0/2
Destination Ports : Gi4/0/3
Encapsulation : Native
Ingress : Enabled, default VLAN = 5
Ingress encap : DOT1Q
Session 2
-----
Type : Local Session
Source Ports :
Both : Gi4/0/8
Destination Ports : Gi4/0/12
Encapsulation : Replicate
Ingress : Enabled, default VLAN = 4
Ingress encap : Untagged
```

The following is sample output from the **show monitor session erspan-source** command:

```
Switch# show monitor session erspan-source

Type : ERSPAN Source Session
Status : Admin Enabled
Source Ports :
RX Only : Gi1/4/33
Destination IP Address : 20.20.163.20
Destination ERSPAN ID : 110
Origin IP Address : 10.10.10.216
IPv6 Flow Label : None
```


show platform software fed switch ip wccp

To display platform-dependent Web Cache Communication Protocol (WCCP) information, use the **show platform software fed switch ip wccp** privileged EXEC command.

```
show platform software fed switch{switch-number|active|standby}ip
wccp{cache-engines |interfaces |service-groups}
```

Syntax Description

switch{*switch_num* | **active** | **standby**} The device for which you want to display information.

- *switch_num*—Enter the switch ID. Displays information for the specified switch.
- **active**—Displays information for the active switch.
- **standby**—Displays information for the standby switch, if available.

cache-engines	Displays WCCP cache engines.
interfaces	Displays WCCP interfaces.
service-groups	Displays WCCP service groups.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1a	This command was introduced.

Usage Guidelines

Use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

This command is available only if your device is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Device# show platform software fed switch 1 ip wccp interfaces
```

```
WCCP Interface Info
```

```
=====
```

```
**** WCCP Interface: Port-channel13 iif_id: 000000000000007c (#SG:3), VRF: 0 Ingress WCCP
****
```

```
port_handle:0x20000f9
```

```
List of Service Groups on this interface:
```

```
* Service group id:90 vrf_id:0 (ref count:24)
```

```
type: Dynamic      Open service      prot: PROT_TCP      l4_type: Dest ports      priority: 35
Promiscuous mode (no ports).
```

```
* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

* Service group id:60 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

**** WCCP Interface: Port-channel14 iif_id: 000000000000007e (#SG:3), VRF: 0 Ingress WCCP
****
port_handle:0x880000fa

List of Service Groups on this interface:
* Service group id:90 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).

* Service group id:70 vrf_id:0 (ref count:24)
type: Dynamic      Open service      prot: PROT_TCP    l4_type: Dest ports    priority: 35
Promiscuous mode (no ports).
<output truncated>
```

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	(Optional) Displays WCCP information only for specified <i>switch-number</i> .
	<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 device is running the IP Services feature set.

The following example displays WCCP interfaces:

```
Device# show platform ip wccp interfaces
```

```
WCCP Interfaces
```

```
**** WCCP Interface Gi1/0/3 iif_id:0x104a60000000087 (#SG:1), vrf:0 Ingress
le_handle:0x565dd208 IPv4 Sw-Label:3, Asic-Label:3
```

```
* Service group id:0 type: Well-known token:126 vrf:0 (ref count:1)
Open service prot: PROT_TCP l4_type: Dest ports priority: 240
port[0]: 80
```

show platform software swspan

To display switched port analyzer (SPAN) information, use the **show platform software swspan** command in privileged EXEC mode.

show platform software swspan {switch} {{{F0 | FP active} counters} | R0 | RP active} {destination sess-id *session-ID* | source sess-id *session-ID*}

Syntax Description

switch	Displays information about the switch.
F0	Displays information about the Embedded Service Processor (ESP) slot 0.
FP	Displays information about the ESP.
active	Displays information about the active instance of the ESP or the Route Processor (RP).
counters	Displays the SWSPAN message counters.
R0	Displays information about the RP slot 0.
RP	Displays information the RP.
destination sess-id <i>session-ID</i>	Displays information about the specified destination session.
source sess-id <i>session-ID</i>	Displays information about the specified source session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced in a release prior to Cisco IOS XE Denali 16.1.1.

Usage Guidelines

If the session number does not exist or if the SPAN session is a remote destination session, the command output will display the following message "% Error: No Information Available."

Examples

The following is sample output from the **show platform software swspan FP active source** command:

```
Switch# show platform software swspan FP active source sess-id 0
```

```
Showing SPAN source detail info
```

```
Session ID : 0
Intf Type : PORT
Port dpidx : 30
PD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
Parent AOM object Id : 118
```

```
Parent AOM object Status : Done
```

```
Session ID : 9
Intf Type : PORT
Port dpidx : 8
PD Sess ID : 0
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 578
AOM Object Status : Done
Parent AOM object Id : 70
Parent AOM object Status : Done
```

The following is sample output from the **show platform software swspan RP active destination** command:

```
Switch# show platform software swspan RP active destination
```

```
Showing SPAN destination table summary info
```

```
Sess-id IF-type IF-id Sess-type
-----
1 PORT 19 Remote
```

snmp-server enable traps

To enable the device to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS), use the **snmp-server enable traps** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps [auth-framework [sec-violation] | bridge | call-home | cluster |
config | config-copy | config-ctid | copy-config | cpu | dot1x | energywise | entity |
envmon | errdisable | event-manager | flash | fru-ctrl | license | mac-notification |
port-security | power-ethernet | rep | snmp | stackwise | storm-control | stpx | syslog
| transceiver | tty | vlan-membership | vlancreate | vlandelete | vstack | vtp ]
no snmp-server enable traps [auth-framework [sec-violation] | bridge | call-home | cluster
| config | config-copy | config-ctid | copy-config | cpu | dot1x | energywise | entity |
envmon | errdisable | event-manager | flash | fru-ctrl | license | mac-notification |
port-security | power-ethernet | rep | snmp | stackwise | storm-control | stpx | syslog
| transceiver | tty | vlan-membership | vlancreate | vlandelete | vstack | vtp ]
```

Syntax Description

auth-framework	(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
sec-violation	(Optional) Enables SNMP camSecurityViolationNotif notifications.
bridge	(Optional) Enables SNMP STP Bridge MIB traps.*
call-home	(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.*
cluster	(Optional) Enables SNMP cluster traps.
config	(Optional) Enables SNMP configuration traps.
config-copy	(Optional) Enables SNMP configuration copy traps.
config-ctid	(Optional) Enables SNMP configuration CTID traps.
copy-config	(Optional) Enables SNMP copy-configuration traps.
cpu	(Optional) Enables CPU notification traps.*
dot1x	(Optional) Enables SNMP dot1x traps.*
energywise	(Optional) Enables SNMP energywise traps.*
entity	(Optional) Enables SNMP entity traps.
envmon	(Optional) Enables SNMP environmental monitor traps.*
errdisable	(Optional) Enables SNMP errdisable notification traps.*
event-manager	(Optional) Enables SNMP Embedded Event Manager traps.
flash	(Optional) Enables SNMP FLASH notification traps.*

fru-ctrl	(Optional) Generates entity field-replaceable unit (FRU) control traps. In a device stack, this trap refers to the insertion or removal of a device in the stack.
license	(Optional) Enables license traps.*
mac-notification	(Optional) Enables SNMP MAC Notification traps.*
port-security	(Optional) Enables SNMP port security traps.*
power-ethernet	(Optional) Enables SNMP power Ethernet traps.*
rep	(Optional) Enables SNMP Resilient Ethernet Protocol traps.
snmp	(Optional) Enables SNMP traps.*
stackwise	(Optional) Enables SNMP stackwise traps.*
storm-control	(Optional) Enables SNMP storm-control trap parameters.*
stpx	(Optional) Enables SNMP STPX MIB traps.*
syslog	(Optional) Enables SNMP syslog traps.
transceiver	(Optional) Enables SNMP transceiver traps.*
tty	(Optional) Sends TCP connection traps. This is enabled by default.
vlan-membership	(Optional) Enables SNMP VLAN membership traps.
vlancreate	(Optional) Enables SNMP VLAN-created traps.
vlandelete	(Optional) Enables SNMP VLAN-deleted traps.
vstack	(Optional) Enables SNMP Smart Install traps.*
vtp	(Optional) Enables VLAN Trunking Protocol (VTP) traps.

Command Default

The sending of SNMP traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The command options marked with an asterisk in the table above have subcommands. For more information on these subcommands, see the Related Commands section below.

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.



Note Though visible in the command-line help strings, the **fru-ctrl**, **insertion**, and **removal** keywords are not supported on the device. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host *host-addr* informs** global configuration command.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable more than one type of SNMP trap:

```
Device(config)# snmp-server enable traps cluster
Device(config)# snmp-server enable traps config
Device(config)# snmp-server enable traps vtp
```


snmp-server enable traps bridge

To generate STP bridge MIB traps, use the **snmp-server enable traps bridge** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps bridge [newroot] [topologychange]
no snmp-server enable traps bridge [newroot] [topologychange]
```

Syntax Description

newroot (Optional) Enables SNMP STP bridge MIB new root traps.

topologychange (Optional) Enables SNMP STP bridge MIB topology change traps.

Command Default

The sending of bridge SNMP traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to send bridge new root traps to the NMS:

```
Device(config)# snmp-server enable traps bridge newroot
```

snmp-server enable traps bulkstat

To enable data-collection-MIB traps, use the **snmp-server enable traps bulkstat** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps bulkstat [collection | transfer]
no snmp-server enable traps bulkstat [collection | transfer]
```

Syntax Description

collection (Optional) Enables data-collection-MIB collection traps.

transfer (Optional) Enables data-collection-MIB transfer traps.

Command Default

The sending of data-collection-MIB traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate data-collection-MIB collection traps:

```
Device(config)# snmp-server enable traps bulkstat collection
```

snmp-server enable traps call-home

To enable SNMP CISCO-CALLHOME-MIB traps, use the **snmp-server enable traps call-home** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps call-home [message-send-fail | server-fail]
no snmp-server enable traps call-home [message-send-fail | server-fail]
```

Syntax Description

message-send-fail (Optional) Enables SNMP message-send-fail traps.

server-fail (Optional) Enables SNMP server-fail traps.

Command Default

The sending of SNMP CISCO-CALLHOME-MIB traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP message-send-fail traps:

```
Device(config)# snmp-server enable traps call-home message-send-fail
```

snmp-server enable traps cef

To enable SNMP Cisco Express Forwarding (CEF) traps, use the **snmp-server enable traps cef** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps cef [inconsistency | peer-fib-state-change | peer-state-change |
resource-failure]
no snmp-server enable traps cef [inconsistency | peer-fib-state-change | peer-state-change |
resource-failure]
```

Syntax Description

inconsistency	(Optional) Enables SNMP CEF Inconsistency traps.
peer-fib-state-change	(Optional) Enables SNMP CEF Peer FIB State change traps.
peer-state-change	(Optional) Enables SNMP CEF Peer state change traps.
resource-failure	(Optional) Enables SNMP CEF Resource Failure traps.

Command Default

The sending of SNMP CEF traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

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 CEF inconsistency traps:

```
Device(config)# snmp-server enable traps cef inconsistency
```

snmp-server enable traps cpu

To enable CPU notifications, use the **snmp-server enable traps cpu** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps cpu [threshold]
no snmp-server enable traps cpu [threshold]
```

Syntax Description	threshold (Optional) Enables CPU threshold notification.				
Command Default	The sending of CPU notifications is disabled.				
Command Modes	Global configuration				
Command History	<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 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:

```
Device(config)# snmp-server enable traps cpu threshold
```

snmp-server enable traps envmon

To enable SNMP environmental traps, use the **snmp-server enable traps envmon** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
no snmp-server enable traps envmon [fan] [shutdown] [status] [supply] [temperature]
```

Syntax Description

fan	(Optional) Enables fan traps.
shutdown	(Optional) Enables environmental monitor shutdown traps.
status	(Optional) Enables SNMP environmental status-change traps.
supply	(Optional) Enables environmental monitor power-supply traps.
temperature	(Optional) Enables environmental monitor temperature traps.

Command Default

The sending of environmental SNMP traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

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 fan traps:

```
Device(config)# snmp-server enable traps envmon fan
```

snmp-server enable traps errdisable

To enable SNMP notifications of error-disabling, use the **snmp-server enable traps errdisable** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]
no snmp-server enable traps errdisable [**notification-rate** *number-of-notifications*]

Syntax Description	notification-rate <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:

```
Device(config)# snmp-server enable traps errdisable notification-rate 2
```

snmp-server enable traps flash

To enable SNMP flash notifications, use the **snmp-server enable traps flash** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps flash [insertion] [removal]
no snmp-server enable traps flash [insertion] [removal]

Syntax Description

insertion (Optional) Enables SNMP flash insertion notifications.

removal (Optional) Enables SNMP flash removal notifications.

Command Default

The sending of SNMP flash notifications is disabled.

Command Modes

Global configuration

Command History

Release

Modification

Cisco IOS XE 3.2SE

This command was introduced.

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP flash insertion notifications:

```
Device(config)# snmp-server enable traps flash insertion
```


snmp-server enable traps isis

To enable intermediate system-to-intermediate system (IS-IS) link-state routing protocol traps, use the **snmp-server enable traps isis** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps isis [errors | state-change]
no snmp-server enable traps isis [errors | state-change]
```

Syntax Description

errors (Optional) Enables IS-IS error traps.

state-change (Optional) Enables IS-IS state change traps.

Command Default

The sending of IS-IS traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate IS-IS error traps:

```
Device(config)# snmp-server enable traps isis errors
```

snmp-server enable traps license

To enable license traps, use the **snmp-server enable traps license** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps license [deploy] [error] [usage]
no snmp-server enable traps license [deploy] [error] [usage]
```

Syntax Description

deploy (Optional) Enables license deployment traps.

error (Optional) Enables license error traps.

usage (Optional) Enables license usage traps.

Command Default

The sending of license traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

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 license deployment traps:

```
Device(config)# snmp-server enable traps license deploy
```

snmp-server enable traps mac-notification

To enable SNMP MAC notification traps, use the **snmp-server enable traps mac-notification** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps mac-notification [change] [move] [threshold]
no snmp-server enable traps mac-notification [change] [move] [threshold]
```

Syntax Description

change (Optional) Enables SNMP MAC change traps.

move (Optional) Enables SNMP MAC move traps.

threshold (Optional) Enables SNMP MAC threshold traps.

Command Default

The sending of SNMP MAC notification traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate SNMP MAC notification change traps:

```
Device(config)# snmp-server enable traps mac-notification change
```

snmp-server enable traps ospf

To enable SNMP Open Shortest Path First (OSPF) traps, use the **snmp-server enable traps ospf** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps ospf [cisco-specific | errors | lsa | rate-limit rate-limit-time
max-number-of-traps | retransmit | state-change]
no snmp-server enable traps ospf [cisco-specific | errors | lsa | rate-limit rate-limit-time
max-number-of-traps | retransmit | state-change]
```

Syntax Description

cisco-specific	(Optional) Enables Cisco-specific traps.
errors	(Optional) Enables error traps.
lsa	(Optional) Enables link-state advertisement (LSA) traps.
rate-limit	(Optional) Enables rate-limit traps.
<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:

```
Device(config)# snmp-server enable traps ospf lsa
```

snmp-server enable traps pim

To enable SNMP Protocol-Independent Multicast (PIM) traps, use the **snmp-server enable traps pim** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps pim [invalid-pim-message] [neighbor-change] [rp-mapping-change]
no snmp-server enable traps pim [invalid-pim-message] [neighbor-change] [rp-mapping-change]
```

Syntax Description

invalid-pim-message (Optional) Enables invalid PIM message traps.

neighbor-change (Optional) Enables PIM neighbor-change traps.

rp-mapping-change (Optional) Enables rendezvous point (RP)-mapping change traps.

Command Default

The sending of PIM SNMP traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable invalid PIM message traps:

```
Device(config)# snmp-server enable traps pim invalid-pim-message
```

snmp-server enable traps port-security

To enable SNMP port security traps, use the **snmp-server enable traps port-security** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps port-security [**trap-rate** *value*]
no snmp-server enable traps port-security [**trap-rate** *value*]

Syntax Description	trap-rate <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:

```
Device(config)# snmp-server enable traps port-security trap-rate 200
```

snmp-server enable traps power-ethernet

To enable SNMP power-over-Ethernet (PoE) traps, use the **snmp-server enable traps power-ethernet** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps power-ethernet {group number | police}
no snmp-server enable traps power-ethernet {group number | police}
```

Syntax Description	group number	Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.
	police	Enables inline power policing traps.

Command Default The sending of power-over-Ethernet SNMP traps is disabled.

Command Modes Global configuration

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

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to enable power-over-Ethernet traps for group 1:

```
Device(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

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 a warmstart SNMP trap:

```
Device(config)# snmp-server enable traps snmp warmstart
```


snmp-server enable traps stackwise

To enable SNMP StackWise traps, use the **snmp-server enable traps stackwise** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps stackwise [GLS] [ILS] [SRLS]
[insufficient-power] [invalid-input-current]
[invalid-output-current] [member-removed] [member-upgrade-notification]
[new-master] [new-member] [port-change] [power-budget-warning] [power-invalid-topology]
[power-link-status-changed] [power-oper-status-changed]
[power-priority-conflict] [power-version-mismatch] [ring-redundant]
[stack-mismatch] [unbalanced-power-supplies] [under-budget] [under-voltage]
no snmp-server enable traps stackwise [GLS] [ILS] [SRLS]
[insufficient-power] [invalid-input-current]
[invalid-output-current] [member-removed] [member-upgrade-notification]
[new-master] [new-member] [port-change] [power-budget-warning] [power-invalid-topology]
[power-link-status-changed] [power-oper-status-changed]
[power-priority-conflict] [power-version-mismatch] [ring-redundant]
[stack-mismatch] [unbalanced-power-supplies] [under-budget] [under-voltage]
```

Syntax	Description
GLS	(Optional) Enables StackWise stack power GLS trap.
ILS	(Optional) Enables StackWise stack power ILS trap.
SRLS	(Optional) Enables StackWise stack power SRLS trap.
insufficient-power	(Optional) Enables StackWise stack power unbalanced power supplies trap.
invalid-input-current	(Optional) Enables StackWise stack power invalid input current trap.
invalid-output-current	(Optional) Enables StackWise stack power invalid output current trap.
member-removed	(Optional) Enables StackWise stack member removed trap.
member-upgrade-notification	(Optional) Enables StackWise member to be reloaded for upgrade trap.
new-master	(Optional) Enables StackWise new master trap.
new-member	(Optional) Enables StackWise stack new member trap.
port-change	(Optional) Enables StackWise stack port change trap.
power-budget-warning	(Optional) Enables StackWise stack power budget warning trap.
power-invalid-topology	(Optional) Enables StackWise stack power invalid topology trap.
power-link-status-changed	(Optional) Enables StackWise stack power link status changed trap.
power-oper-status-changed	(Optional) Enables StackWise stack power port oper status changed trap.
power-priority-conflict	(Optional) Enables StackWise stack power priority conflict trap.

power-version-mismatch	(Optional) Enables StackWise stack power version mismatch discovered trap.
ring-redundant	(Optional) Enables StackWise stack ring redundant trap.
stack-mismatch	(Optional) Enables StackWise stack mismatch trap.
unbalanced-power-supplies	(Optional) Enables StackWise stack power unbalanced power supplies trap.
under-budget	(Optional) Enables StackWise stack power under budget trap.
under-voltage	(Optional) Enables StackWise stack power under voltage trap.

Command Default The sending of SNMP StackWise traps is disabled.

Command Modes Global configuration

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

Usage Guidelines Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate StackWise stack power GLS traps:

```
Device(config)# snmp-server enable traps stackwise GLS
```

snmp-server enable traps storm-control

To enable SNMP storm-control trap parameters, use the **snmp-server enable traps storm-control** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps storm-control {trap-rate number-of-minutes}
no snmp-server enable traps storm-control {trap-rate}
```

Syntax Description	trap-rate <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:

```
Device(config)# snmp-server enable traps storm-control trap-rate 10
```

snmp-server enable traps stpx

To enable SNMP STPX MIB traps, use the **snmp-server enable traps stpx** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
no snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]
```

Syntax Description

inconsistency (Optional) Enables SNMP STPX MIB inconsistency update traps.

loop-inconsistency (Optional) Enables SNMP STPX MIB loop inconsistency update traps.

root-inconsistency (Optional) Enables SNMP STPX MIB root inconsistency update traps.

Command Default

The sending of SNMP STPX MIB traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note

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 STPX MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```

snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the **snmp-server enable traps transceiver** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps transceiver {all}
no snmp-server enable traps transceiver {all}
```

Syntax Description

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 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 set all SNMP transceiver traps:

```
Device(config)# snmp-server enable traps transceiver all
```

snmp-server enable traps vrfmib

To allow SNMP vrfmib traps, use the **snmp-server enable traps vrfmib** command in global configuration mode. Use the **no** form of this command to return to the default setting.

snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]
no snmp-server enable traps vrfmib [**vnet-trunk-down** | **vnet-trunk-up** | **vrf-down** | **vrf-up**]

Syntax Description

vnet-trunk-down (Optional) Enables vrfmib trunk down traps.

vnet-trunk-up (Optional) Enables vrfmib trunk up traps.

vrf-down (Optional) Enables vrfmib vrf down traps.

vrf-up (Optional) Enables vrfmib vrf up traps.

Command Default

The sending of SNMP vrfmib traps is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.



Note Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

Examples

This example shows how to generate vrfmib trunk down traps:

```
Device(config)# snmp-server enable traps vrfmib vnet-trunk-down
```

snmp-server enable traps vstack

To enable SNMP smart install traps, use the **snmp-server enable traps vstack** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
snmp-server enable traps vstack [addition] [failure] [lost] [operation]
no snmp-server enable traps vstack [addition] [failure] [lost] [operation]
```

Syntax Description

addition (Optional) Enables client added traps.

failure (Optional) Enables file upload and download failure traps.

lost (Optional) Enables client lost trap.

operation (Optional) Enables operation mode change traps.

Command Default

The sending of SNMP smart install traps is disabled.

Command Modes

Global configuration

Command History

Release

Cisco IOS XE 3.2SE

Modification

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:

```
Device(config)# snmp-server enable traps vstack addition
```

snmp-server engineID

To configure a name for either the local or remote copy of SNMP, use the **snmp-server engineID** command in global configuration mode.

```
snmp-server engineID {local engineid-string | remote ip-address [udp-port port-number]
engineid-string}
```

Syntax Description	<p>local <i>engineid-string</i> Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.</p> <p>remote <i>ip-address</i> Specifies the remote SNMP copy. Specify the <i>ip-address</i> of the device that contains the remote copy of SNMP.</p> <p>udp-port <i>port-number</i> (Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.</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	None				

Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```


snmp-server host

To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** global configuration command on the device. Use the **no** form of this command to remove the specified host.

```
snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c | 3
{auth | noauth | priv} } ] {community-string [notification-type] }
no snmp-server host {host-addr} [vrf vrf-instance] [informs | traps] [version {1 | 2c |
3 {auth | noauth | priv} } ] {community-string [notification-type] }
```

Syntax Description

<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.
 - **stp**—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.
-

Command Default

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

**Note**

Though visible in the command-line help strings, the **fru-ctrl** keyword is not supported.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again, so that informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the device to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the device does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

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:

```
Device(config)# snmp-server community comaccess ro 10
Device(config)# snmp-server host 172.20.2.160 comaccess
Device(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name myhost.cisco.com. The community string is defined as comaccess:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the device to send all traps to the host myhost.cisco.com by using the community string public:

```
Device(config)# snmp-server enable traps
Device(config)# snmp-server host myhost.cisco.com public
```

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

source (ERSPAN)

To configure the Encapsulated Remote Switched Port Analyzer (ERSPAN) source interface or VLAN, and the traffic direction to be monitored, use the **source** command in ERSPAN monitor source session configuration mode. To disable the configuration, use the **no** form of this command.

```
source {interface type number | vlan vlan-ID}[, | - | both | rx | tx]
```

Syntax Description	
interface <i>type number</i>	Specifies an interface type and number.
vlan <i>vlan-ID</i>	Associates the ERSPAN source session number with VLANs. Valid values are from 1 to 4094.
,	(Optional) Specifies another interface.
-	(Optional) Specifies a range of interfaces.
both	(Optional) Monitors both received and transmitted ERSPAN traffic.
rx	(Optional) Monitors only received traffic.
tx	(Optional) Monitors only transmitted traffic.

Command Default Source interface or VLAN is not configured.

Command Modes ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines You cannot include source VLANs and filter VLANs in the same session.

Examples The following example shows how to configure ERSPAN source session properties:

```
Switch(config)# monitor session 2 type erspan-source
Switch(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

Related Commands	Command	Description
	monitor session type erspan-source	Configures a local ERSPAN source session.

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

```
Device(config-template)# switchport mode access
```

switchport voice vlan

To specify to forward all voice traffic through the specified VLAN, use the **switchport voice vlan** command in template configuration mode. Use the **no** form of this command to return to the default setting.

```
switchport voice vlan vlan_id
no switchport voice vlan
```

Syntax Description	switchport voice vlan <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	This command was introduced.

Examples

This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Device(config-template)# switchport voice vlan 20
```




PART **IX**

Programmability

- [Programmability, on page 539](#)



Programmability

- [boot ipxe, on page 540](#)
- [boot manual, on page 541](#)
- [boot system, on page 542](#)
- [default boot, on page 543](#)
- [install, on page 544](#)
- [show install, on page 548](#)
- [dig, on page 550](#)
- [mlog, on page 552](#)
- [net-debug, on page 553](#)
- [net-dhcp, on page 555](#)
- [net6-dhcp, on page 556](#)
- [net-show , on page 557](#)
- [net6-show, on page 558](#)
- [net-tcp-bufs, on page 559](#)
- [net-tcp-mss, on page 560](#)
- [ping, on page 561](#)
- [ping4, on page 562](#)
- [ping6, on page 563](#)

boot ipxe

To configure the iPXE boot, use the **boot ipxe** command in global configuration mode. To disable the configuration, use the **no** form of this command.

boot ipxe{**forever** | **timeout** *seconds*}**switch** *switch-number*
no boot ipxe{**forever** | **timeout** *seconds*}**switch** *switch-number*

Syntax Description	Parameter	Description
	forever	Attempts iPXE boot forever.
	timeout <i>seconds</i>	Configures a timeout in seconds for iPXE network boot. Valid values are from 1 to 2147483647.
	switch <i>switch-number</i>	Enables iPXE boot for switches in the stack. Valid values are from 0 to 9.

Command Default Device boot is the default.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines iPXE is an open source implementation of Preboot eXecution Environment (PXE). The bootloaders boot an image located on an HTTP, FTP, or a TFTP server.

If the **forever** keyword is configured, the switch sends Dynamic Host Control Protocol (DHCP) requests forever. If the **timeout** keyword is configured, DHCP requests are sent for the specified amount of time, and when the timeout expires, the switch reverts to device boot.

Example

The following example shows how to configure an iPXE boot timeout for switch 2:

```
Device(config)# boot ipxe timeout 240 switch 2
```

Command	Description
default boot	Modifies the default boot system parameters.

boot manual

To configure manual boot, use the **boot manual** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
boot manual switch switch-number
no boot manual switch switch-number
```

Syntax Description

switch *switch-number* Configures manual boot for the switches in the stack.

Command Default

Manual boot is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines

When manual boot is disabled, and the switch reloads, the boot process starts automatically. When manual boot is disabled, the bootloader determines whether to execute a device boot or a network boot based on the configured value of the iPXE ROMMON variable.

Example

The following example shows how to configure manual boot for switch 2:

```
Device(config)# boot manual switch 2
```

boot system

To enable a system image boot, use the **boot system** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
boot system switch {all | number} {flash: | ftp: | http: | tftp:}
```

```
no boot system [{switch | {all | number}}] [{flash: | ftp: | http: | tftp: | }]
```

Syntax Description	
flash:	Specifies the flash filesystem to boot an image.
ftp:	Specifies an FTP location to boot an image.
http:	Specifies an HTTP location to boot an image.
tftp:	Specifies a TFTP location to boot an image.
switch <i>number</i>	Enables booting for switches in a stack. Valid values are from 0 to 9.

Command Modes	
	Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Usage Guidelines	
	You can either use an IPv4 or an IPv6 address for the remote FTP/HTTP/TFTP servers.
	For an IPv6 address, you must enter the IPv6 address inside square brackets (as per RFC 2732); if not the device will not boot.

Example

The following example shows how to boot an image file from an IPv4 HTTP server:

```
Device(config)# boot system switch 1 http://192.0.2.42/image-filename
```

The following example shows how to boot an image file from an IPv6 HTTP server:

```
Device(config)# boot system switch 1 http://[2001:db8::1]/image-filename
```

default boot

To modify the default boot system parameters, use the **default boot** command in global configuration mode.

default boot {**ipxe** {**forever** | | **timeout** | **seconds**} | | **manual** | | **system** {**flash:** | | **ftp:** | | **http:** | | **tftp:**}} **switch** *number*

Syntax Description	Parameter	Description
	ipxe	Enables iPXE boot.
	forever	Configures forever boot.
	timeout <i>seconds</i>	Configures a boot timeout in seconds. Valid values are from 1 to 2147483647.
	manual	Enables manual boot.
	system	Enables a system image boot.
	flash:	Specifies the flash filesystem to boot an image.
	ftp:	Specifies an FTP location to boot an image.
	http:	Specifies an HTTP location to boot an image.
	tftp:	Specifies a TFTP location to boot an image.
	switch <i>number</i>	Enables booting for switches in a stack. Valid values are from 0 to 9.

Command Default Device boot is the default.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	The command was introduced.

Usage Guidelines You can either use the **no boot ipxe** or the **default boot ipxe** command to configure device boot.

Example

The following example shows how to enable the default boot mode:

```
Device(config)# default boot ipxe
```

Related Commands	Command	Description
	boot ipxe	Configures iPXE boot.

install

To install Software Maintenance Upgrade (SMU) packages, use the **install** command in privileged EXEC mode.

```
install {activate | file {bootflash: | flash: | webui:} [{prompt-level {all | none}}]} | add file {bootflash:
| flash: | ftp: | http: | https: | rcp: | scp: | tftp: | webui:} [{activate [{prompt-level {all | none}}]}]
| commit | deactivate file {bootflash: | flash: | webui:} [{prompt-level {all | none}}]} | remove {file
{bootflash: | flash: | ftp: | http: | https: | rcp: | scp: | tftp: | webui:} | inactive } | rollback to {base
| committed | id {install-ID }}}
```

Syntax Description

activate	Validates whether the SMU is added through the install add command, and restarts the Netconf processes. This keyword runs a compatibility check, updates package status, and if the package can be restarted, it triggers post-install scripts to restart the necessary processes, or triggers a reload for non-restartable packages.
file	Specifies the package to be activated.
{bootflash: flash: http: https: rcp: scp: tftp:webui:}	Specifies the location of the installed package.
prompt-level {all none}	(Optional) Prompts the user about installation activities. For example, the activate keyword, automatically triggers a reload for packages that require a reload. Before activating the package, a message will prompt users as to whether they want to continue. The all keyword allows you to enable prompts. The none keyword disables prompts.
add	Copies files from a remote location (via FTP, TFTP) to a device and performs Software Maintenance Upgrade (SMU) compatibility check for the platform and image versions. This keyword runs base compatibility checks to ensure that a specified package is supported on a platform. It also adds an entry in the package file, so that the status can be monitored and maintained.
{http: https: rcp: scp: tftp:}	Specifies the package to be added.

commit	Makes SMU changes persistent over reloads. You can do a commit after activating a package, while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.
deactivate	Deactivates an installed package. Deactivating a package also updates the package status and triggers a process restart or a reload.
remove	Remove installed packages. The package file is removed from the file system. The remove keyword can only be used on packages that are currently inactive.
inactive	Removes all inactive packages from the device.
rollback	Rollbacks the SMU package to the base version, the last committed version, or a known commit ID, and restarts Netconf processes.
to base	Returns to the base image.
committed	Returns to the installation state when the last commit operation was performed.
id <i>install-ID</i>	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

Command Default Packages are not installed.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package contain a minimal set of files for patching the release along with some metadata that describes the contents of the package.

Packages msut be added prior to activating the SMU.

A package must be deactivated, before it is removed from the bootflash. A removed packaged must be added again.

Example

The following example shows how to add an install package on a device:

```

Device# install add file tftp://172.16.0.1/tftpboot/folder1/
isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin

install_add: START Sun Feb 26 05:57:04 UTC 2017
Downloading file
tftp://172.16.0.1/tftpboot/folder1/isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Finished downloading file
tftp://172.16.0.1/tftpboot/folder1/isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
to bootflash:isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
SUCCESS: install_add /bootflash/isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
Device#

```

The following example shows how to activate an install package:

```

Device# install activate file bootflash:isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin

install_activate: START Sun Feb 26 05:58:41 UTC 2017
DMP package.
Netconf processes stopped
SUCCESS: install_activate /bootflash/isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Sun Feb 26 05:58:58 UTC 2017*Feb 26 05:58:47.655: %DMI-4-CONTROL_SOCKET_CLOSED:
SIP0: nescd: Confd control socket closed Lost connection to Confd (45): EOF on socket to
Confd.
*Feb 26 05:58:47.661: %DMI-4-SUB_READ_FAIL: SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to Confd (45):
EOF on socket to Confd.
*Feb 26 05:58:47.667: %DMI-4-CONTROL_SOCKET_CLOSED: SIP0: syncfd:
Confd control socket closed Lost connection to Confd (45): EOF on socket to Confd.
*Feb 26 05:59:43.269: %DMI-5-SYNC_START: SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 05:59:44.624: %DMI-5-SYNC_COMPLETE: SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
Device#

```

The following example shows how to commit an installed package:

```

Device# install commit

install_commit: START Sun Feb 26 06:46:48 UTC 2017
SUCCESS: install_commit Sun Feb 26 06:46:52 UTC 2017

```

The following example shows how to rollback to the base SMU package:

```

Device# install rollback to base

install_rollback: START Sun Feb 26 06:50:29 UTC 2017
7 install_rollback: Restarting impacted processes to take effect
7 install_rollback: restarting confd

*Feb 26 06:50:34.957: %DMI-4-CONTROL_SOCKET_CLOSED: SIP0: syncfd:
Confd control socket closed Lost connection to Confd (45): EOF on socket to Confd.
*Feb 26 06:50:34.962: %DMI-4-CONTROL_SOCKET_CLOSED: SIP0: nescd:
Confd control socket closed Lost connection to Confd (45): EOF on socket to Confd.
*Feb 26 06:50:34.963: %DMI-4-SUB_READ_FAIL: SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to Confd (45):
EOF on socket to Confd.Netconf processes stopped
7 install_rollback: DMP activate complete
SUCCESS: install_rollback Sun Feb 26 06:50:41 UTC 2017
*Feb 26 06:51:28.901: %DMI-5-SYNC_START: SIP0: syncfd:
External change to running configuration detected.

```

```
The running configuration will be synchronized to the NETCONF running data store.  
*Feb 26 06:51:30.339: %DMI-5-SYNC_COMPLETE: SIP0: syncfd:  
The running configuration has been synchronized to the NETCONF running data store.
```

Related Commands

Command	Description
show install	Displays information about install packages.

show install

To display information about install packages, use the **show install** command in privileged EXEC mode.

show install {**active** | **committed** | **inactive** | **log** | **package** {**bootflash:** | **flash:** | **webui:**} | **rollback** | **summary** | **uncommitted**}

Syntax Description		
active		Displays information about active packages.
committed		Displays package activations that are persistent.
inactive		Displays inactive packages.
log		Displays entries stored in the logging installation buffer.
package		Displays metadata information about the package, including description, restart information, components in the package, and so on.
{ bootflash: flash: webui: }		Specifies the location of the install package.
rollback		Displays the software set associated with a saved installation.
summary		Displays information about the list of active, inactive, committed, and superseded packages.
uncommitted		Displays package activations that are nonpersistent.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines Use the show commands to view the status of the install package.

Example

The following is sample output from the **show install package** command:

```
Device# show install package bootflash:isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
```

```
Name: isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Version: 16.5.1.0.199.1484082952..Everest
Platform: ISR4300
Package Type: dmp
Defect ID: CSCxxxxxxx
Package State: Added
Supersedes List: {}
Smu ID: 1
```

Device#

The following is sample output from the **show install summary** command:

```
Device# show install summary

Active Packages:
bootflash:isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Inactive Packages:
No packages
Committed Packages:
bootflash:isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Uncommitted Packages:
No packages
Device#
```

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

Table 29: show install summary Field Descriptions

Field	Description
Active Packages	Name of the active install package.
Inactive Packages	List of inactive packages.
Committed Packages	Install packages that have saved or committed changes to the harddisk, so that the changes become persistent across reloads.
Uncommitted Packages	Intall package activations that are nonpersistent.

The following is sample output from the **show install log** command:

```
Device# show install log
[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS /bootflash/isr4300-universalk9.16.05.01.CSCxxxxxxx.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
Device#
```

Related Commands

Command	Description
install	Installs SMU packages.

dig

To do a lookup of the Domain Name System (DNS) server, use the **dig** command in rommon mode.

```
dig hostname {v4 v6} [{dns-server-address}]
```

Syntax Description	<i>hostname</i>	DNS host name
	<i>v4</i>	IPv4 address.
	<i>v6</i>	IPv6 address.
	<i>dns-server-address</i>	(Optional) DNS Server IP address.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.
Usage Guidelines	This command does a look up of the DNS name and displays the IP/IPv6 address of the DNS server.	

Example

The following is sample output from the **dig** *hostname* command:

```
Device: dig example.org

DNS lookup using 2001:DB8::1
addr = 2001:DB8:0000:0000:0000:0000:0000:0001
```

The following is sample output from the **dig** *hostname v4* command:

```
Device: dig example.org v4

DNS lookup using 10.29.27.5
addr = 172.16.0.1
```

The following is sample output from the **dig** *hostname v4 dns-server-address* command:

```
Device: dig example.org v4 10.29.27.5

DNS lookup using 10.29.27.5
addr = 172.16.0.1
```

The following is sample output from the **dig** *hostname v6* command:

```
Device: dig example.org v6

DNS lookup using 2001:DB::1
addr = 2001:DB8:0000:0000:0000:0000:0000:0001
```

Related Commands

Command	Description
net-debug	Displays or changes the network debug values.

mlog

To direct log messages to a memory buffer instead of the serial port, use the **mlog** command in rommon mode.

mlog [{show | reset | ctrl [{on | off | toggle}]]

Syntax Description

show	(Optional) Displays memory log messages.
reset	(Optional) Resets the logging of messages to the memory log.
ctrl	(Optional)
on	(Optional)
off	(Optional)
toggle	(Optional)

Command Modes

Rommon

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines

This command directs protocol log (that is all logs controlled by the **net-debug** command) messages to a memory buffer instead of the serial port.

With memory logging, log messages are displayed after a test is run. For example, HTTP debugs can be enabled through memory logging. Log messages are displayed in the memory buffer after running a copy from `http://server/name to null: command`.

Example

The following example shows how to direct log messages to the memory buffer:

```
Device: mlog show
```

Related Commands

Command	Description
net-debug	Displays or changes the network debug values.

net-debug

To display or change the network debug values use the **net-debug** command in rommon mode.

net-debug [{*new-value*}]

Syntax Description	<i>new-value</i>	(Optional) New debug value to use.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines This command enables or disables log levels for each of the following functional areas:

- Domain Name System (DNS)
- Dynamic Host Control Protocol (DHCP)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- IP
- TCP
- UDP
- Uniform Resource Identifier (URI)

Example

The following is sample output from the **net-debug** command:

```
Device: net-debug

ether: 0
 ip: 0
 dhcp: 0
 udp: 0
 tcp: 0
 http: 0
 dns: 0
 uri: 0
 t/ftp: 2
 ip6: 0
 dhcp6: 0:000 200 000 000
```

Related Commands

Command	Description
mlog	Directs log messages to a memory buffer instead of the serial port.

net-dhcp

To initiate an IPv4 Dynamic Host Control Protocol (DHCP) request for remote configuration, use the **net-dhcp** command in rommon mode.

net-dhcp [{**timeout**}]

Syntax Description	timeout	(Optional) Timeout in seconds.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.
Usage Guidelines	This command initiates an IPv4 DHCP request and processes the reply.	

Example

The following example shows how to enable the **net-dhcp** command:

Device: **net-dhcp**

Related Commands	Command	Description
	net-debug	Displays or changes the network debug values.
	net-show	Displays network parameters.
	net6-dhcp	Initiates an IPv6 DHCP request for remote configuration.

net6-dhcp

To initiate an IPv6 Dynamic Host Control Protocol (DHCP) request for remote configuration, use the **net6-dhcp** command in rommon mode.

net6-dhcp [{timeout}]

Syntax Description	timeout	(Optional) Timeout in seconds.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.
Usage Guidelines	You can change the timeout by specifying a time in seconds	

Example

The following example shows how to enable the **net6-dhcp** command:

Device: **net6-dhcp**

Related Commands	Command	Description
	net-debug	Displays or changes the network debug values.
	net-dhcp	Initiates an IPv4 DHCP request and processes the reply.
	net-show	Displays network parameters.

net-show

To display network parameters, use the **net-show** command in rommon mode.

net-show

This command has no arguments or keywords.

Command Modes

Rommon

Command History

Release	Modification
Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines

This command displays network configuration such as IP address, gateway, MAC address and so on.

Example

The following is sample output from the **net-show** command:

```
Device: net-show
Network params:
IPv4:
    ip addr 10.29.27.150
    netmask 255.255.0.0
    gateway 10.29.0.1
IPv6:
link-local addr fe80::366f:90ff:feb8:cb80
site-local addr fec0::366f:90ff:feb8:cb80
    DHCP addr 2001:dead:beef:cafe::9999
    router addr fe80::7ada:6eff:fe13:8580
    SLAAC addr 2001:dead:beef:cafe:366f:90ff:feb8:cb80 /64
    SLAAC addr f00d::366f:90ff:feb8:cb80 /64
    SLAAC addr feed::366f:90ff:feb8:cb80 /64
Common:
    macaddr 34:6f:90:b8:cb:80
    dns 2001:dead:beef:cafe::5
    bootfile http://www.example.org/ed10m
    domain ip6.example.org
```

Command	Description
net6-show	Displays IPv6 network parameters.

net6-show

To display IPv6 network parameters, use the **net6-show** command in rommon mode.

net6-show

This command has no arguments or keywords.

Command Modes Rommon

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines

Example

The following is sample output from the **net6-show** command:

```
Device: net6-show

switch: net6-show
IP6 addresses
link-local addr fe80::366f:90ff:feb8:cb80
site-local addr fec0::366f:90ff:feb8:cb80
    DHCP addr 2001:dead:beef:cafe::9999
    router addr fe80::7ada:6eff:fe13:8580
    SLAAC addr 2001:dead:beef:cafe:366f:90ff:feb8:cb80 /64
    SLAAC addr f00d::366f:90ff:feb8:cb80 /64
    SLAAC addr feed::366f:90ff:feb8:cb80 /64
--
    null addr ::
    all-nodes addr ff02::1
all-routers addr ff02::2
    all-dhcp addr ff02::1:2
    Slct-node addr ff02::1:ffb8:cb80
    ll mmac addr 33:33:00:00:00:01
    sl mmac addr 33:33:00:00:00:02
    sn mmac addr 33:33:ff:b8:cb:80
    dhcp mmac addr 33:33:ff:00:99:99
router mac addr 78:da:6e:13:85:80

IP6 neighbour table
0: ip6 fec0::366f:90ff:feb8:cb80 MAC 34:6f:90:b8:cb:80
1: ip6 fe80::366f:90ff:feb8:cb80 MAC 34:6f:90:b8:cb:80
2: ip6 fe80::7ada:6eff:fe13:8580 MAC 78:da:6e:13:85:80
3: ip6 2001:dead:beef:cafe::5 MAC 30:f7:0d:08:7e:bd
4: ip6 fe80::32f7:dff:fe08:7ebd MAC 30:f7:0d:08:7e:bd
```

Related Commands

Command	Description
net-show	Displays network parameters.

net-tcp-bufs

To display TCP buffers, use the **net-tcp-bufs** command in rommon mode.

net-tcp-bufs [{*mss*}]

Syntax Description	<i>mss</i>	(Optional) The Maximum Segment Size (MSS) of TCP buffers.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.
Usage Guidelines	You can set the MSS of TCP buffers using the <i>mss</i> argument.	

Example

The following is sample output from the **net-tcp-bufs** command:

```
Device: net tcp-bufs
```

```
tcp_num_bufs 4
```

Related Commands	Command	Description
	net-tcp-mss	View or set the TCP MSS.

net-tcp-mss

To view or set the TCP Maximum Segment Size (MSS), use the **net-tcp-mss** command in rommon mode.

net-tcp-mss [*mss*]

Syntax Description	<i>mss</i>	(Optional) The Maximum Segment Size (MSS) of TCP buffers.
Command Modes	Rommon	
Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.
Usage Guidelines	Use the <i>mss</i> argument to change the MSS size.	

Example

The following is sample output from the **net-tcp-mss** command:

```
Device: net-tcp-mss
switch: net-tcp-mss
tcp_segment_size 1024
```

The following is sample output from the **net-tcp-mss mss** command:

```
Device: net-tcp-mss 700
switch: net-tcp-mss 700
tcp_segment_size 700
```

Related Commands

Command	Description
net-tcp-bufs	Displays TCP buffers.

ping

To diagnose basic network connectivity, use the **ping** command in rommon mode.

ping [{*host_ip_address*}] [{*retries*}]

Syntax Description	<i>host_ip_address</i>	(Optional) IP address of the host.
	<i>retries</i>	(Optional) Number of retries.

Command Modes	Rommon
----------------------	--------

Command History	Release	Modification
		Cisco IOS XE Everest 16.5.1

Usage Guidelines

The **ping** and **ping4** commands are the same.

The **ping** command is a very common method for troubleshooting the accessibility of devices

A timeout is implemented at the bootloader device prompt, that allows the bootloader to poll the TCP stack every 200 ms. As a result, the bootloader may take up to 200 ms to respond to pings. However, when the bootloader is downloading a file, and thus actively polling for new packets, it responds to ping quickly.

Example

The following is sample output from the **ping** command:

```
Device: ping 10.29.27.5
Ping 10.29.27.5 with 32 bytes of data ...
Host 10.29.27.5 is alive.
```

The following is sample output from the **ping host_ip_address retries** command:

```
Device: ping 10 6.29.27.5 6
Ping 10.29.27.5 with 32 bytes of data ... reply received in 0 ms
Ping 10.29.27.5 with 32 bytes of data ... reply received in 0 ms
Ping 10.29.27.5 with 32 bytes of data ... reply received in 0 ms
Ping 10.29.27.5 with 32 bytes of data ... reply received in 1 ms
Ping 10.29.27.5 with 32 bytes of data ... reply received in 0 ms
Ping 10.29.27.5 with 32 bytes of data ... reply received in 0 ms
```

Related Commands	Command	Description
	ping4	Diagnoses basic network connectivity.
	ping6	Determines the network connectivity to another device using IPv6 addressing.

ping4

To diagnose basic network connectivity, use the **ping4** command in rommon mode.

ping4 [{*host_ip_address* }][{*retries*}]

Syntax Description		
	<i>host_ip_address</i>	(Optional) IP address of the host to be pinged.
	<i>retries</i>	(Optional) Number of retries.

Command Modes Rommon

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines The **ping** and **ping4** commands are the same

A timeout is implemented at the bootloader device prompt, that allows the bootloader to poll the TCP stack every 200 ms. As a result, the bootloader may take up to 200 ms to respond to pings. However, when the bootloader is downloading a file, and thus actively polling for new packets, it responds to ping quickly.

Example

The following is sample output from the **ping4** *host_ip_address* command:

```
Device: ping4 10.29.27.5

Ping 10.29.27.5 with 32 bytes of data ...
Host 10.29.27.5 is alive.
```

Related Commands	Command	Description
	ping	Diagnoses basic network connectivity.
	ping6	Determines the network connectivity to another device using IPv6 addressing.

ping6

To determine the network connectivity to another device using IPv6 addressing, use the **ping6** command, rommon mode.

ping6 [*host*] [*repeats*] [*len*]

Syntax Description	<i>host</i>	(Optional) IP address of the host to be pinged.
	<i>repeats</i>	(Optional) Number of times to repeat the ping.

Command Modes Rommon

Command History	Release	Modification
	Cisco IOS XE Everest 16.5.1	This command was introduced.

Usage Guidelines A timeout is implemented at the bootloader device prompt, that allows the bootloader to poll the TCP stack every 200 ms. As a result, the bootloader may take up to 200 ms to respond to pings. However, when the bootloader is downloading a file, and thus actively polling for new packets, it responds to ping quickly.

Example

The following is sample output from the **ping6 host retries len** command:

```
Device: ping6 2001:dead:beef:cafe::5 6 1000

Ping host 2001:dead:beef:cafe::5, 6 times, 1000 bytes
Pinging 2001:dead:beef:cafe::5 ... reply in 0 ms
Pinging 2001:dead:beef:cafe::5 ... reply in 1 ms
Pinging 2001:dead:beef:cafe::5 ... reply in 1 ms
Pinging 2001:dead:beef:cafe::5 ... reply in 0 ms
Pinging 2001:dead:beef:cafe::5 ... reply in 0 ms
Pinging 2001:dead:beef:cafe::5 ... reply in 0 ms
```

Related Commands	Command	Description
	ping	Diagnoses basic network connectivity.
	ping4	Diagnoses basic network connectivity.



PART **X**

QoS

- [Auto-QoS, on page 567](#)
- [QoS , on page 609](#)



Auto-QoS

This chapter contains the following auto-QoS commands:

- [auto qos classify](#), on page 568
- [auto qos trust](#), on page 574
- [auto qos video](#), on page 582
- [auto qos voip](#) , on page 593
- [debug auto qos](#), on page 606
- [show auto qos](#) , on page 607

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 device, 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 30: 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 device 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 device 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 device 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:

```
Device(config)# interface gigabitEthernet1/0/6
Device(config-if)# auto qos classify police
Device(config-if)# end
Device# 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 device, 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 31: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ³ BPDU ⁴ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ⁵	46	24, 26	48	56	34	–	
CoS ⁶	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)

³ STP = Spanning Tree Protocol

⁴ BPDU = bridge protocol data unit

⁵ DSCP = Differentiated Services Code Point

⁶ CoS = class of service

Table 32: 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 device 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 device 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.

```
Device(config)# interface gigabitEthernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# 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.

```

Device(config)# interface GigabitEthernet1/0/18
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device#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 device, 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 device 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 device 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 device 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 33: Traffic Types, Packet Labels, and Queues

	VOIP Data Traffic	VOIP Control Traffic	Routing Protocol Traffic	STP ⁷ BPDU ⁸ Traffic	Real-Time Video Traffic	All Other Traffic	
DSCP ⁹	46	24, 26	48	56	34	—	
CoS ¹⁰	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)

⁷ STP = Spanning Tree Protocol

⁸ BPDU = bridge protocol data unit

⁹ DSCP = Differentiated Services Code Point

¹⁰ CoS = class of service

Table 34: 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:

```

Device(config)# interface gigabitEthernet1/0/12
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# 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:

```

Device(config)# interface GigabitEthernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# 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.

```

Device(config)# interface GigabitEthernet1/0/7
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# 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 device, 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 device, the network interior, and edge devices that can classify incoming traffic for QoS.

Auto-QoS configures the device for VoIP with Cisco IP phones on device 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 device 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 device 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 device enables the trusted boundary feature. The device 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 device 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 device 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 device 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 device 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 device 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 device 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 device or routed port, the device 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 device configures egress queues on the port according to the settings in this table.

Table 35: 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:

```
Device(config)# interface gigabitEthernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# 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:

```

Device(config)# interface gigabitEthernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# 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:

```

Device(config)# interface gigabitEthernet1/0/20
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# 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 device stack, it is enabled only on the active device. To enable debugging on a stack member, you can start a session from the active device 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 device to enable debugging on a member device without first starting a session.

Examples

This example shows how to display the QoS configuration that is automatically generated when auto-QoS is enabled:

```
Device# debug auto qos
AutoQoS debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface gigabitethernet2/0/1
Device(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:

```
Device# 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:

```
Device# 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:

```
Device# 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:

```
Device# show auto qos interface gigabitethernet3/0/1
AutoQoS is disabled
```




QoS

This chapter contains the following QoS commands:

- [class](#), on page 610
- [class-map](#), on page 613
- [match \(class-map configuration\)](#), on page 615
- [match non-client-nrt](#), on page 618
- [policy-map](#), on page 619
- [priority](#), on page 621
- [queue-buffers ratio](#), on page 623
- [queue-limit](#), on page 624
- [service-policy \(Wired\)](#), on page 626
- [set](#), on page 628
- [show class-map](#), on page 634
- [show platform hardware fed switch](#), on page 635
- [show platform software fed switch qos](#), on page 638
- [show platform software fed switch qos qsb](#), on page 639
- [show policy-map](#), on page 642
- [trust device](#), on page 644

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 628
- **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.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Device(config-pmap-c)# exit
```

This example shows how to configure a default traffic class to a policy map. It also shows how the default traffic class is automatically placed at the end of policy-map pm3 even though **class-default** was configured first:

```
Device# configure terminal
Device(config)# class-map cm-3
Device(config-cmap)# match ip dscp 30
Device(config-cmap)# exit

Device(config)# class-map cm-4
Device(config-cmap)# match ip dscp 40
Device(config-cmap)# exit

Device(config)# policy-map pm3
Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-3
Device(config-pmap-c)# set dscp 4
Device(config-pmap-c)# exit

Device(config-pmap)# class cm-4
Device(config-pmap-c)# set precedence 5
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device# show policy-map pm3
Policy Map pm3
  Class cm-3
    set dscp 4
  Class cm-4
    set precedence 5
  Class class-default
```

```
set dscp af11
```

class-map

To create a class map to be used for matching packets to the class whose name you specify and to enter class-map configuration mode, use the **class-map** command in global configuration mode. Use the **no** form of this command to delete an existing class map and to return to global or policy map configuration mode.

```
class-map class-map name {match-any | match-all}
no class-map class-map name {match-any | match-all}
```

Syntax Description	match-any	(Optional) Perform a logical-OR of the matching statements under this class map. One or more criteria must be matched.
	match-all	(Optional) Performs a logical-AND of the matching statements under this class map. All criterias must match.
	<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.
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.	
	<p>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.</p> <p>After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <p>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).</p>	
Examples	This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:	

```
Device(config)# access-list 103 permit ip any any dscp 10  
Device(config)# class-map class1  
Device(config-cmap)# match access-group 103  
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match (class-map configuration)

To define the match criteria to classify traffic, use the **match** command in class-map configuration mode. Use the **no** form of this command to remove the match criteria.

```
match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
no match {access-group {name acl-name acl-index} | class-map class-map-name | cos cos-value | dscp
dscp-value | [ip] dscp dscp-list | [ip] precedence ip-precedence-list | precedence
precedence-value1...value4 | qos-group qos-group-value | vlan vlan-id}
```

Syntax Description		
access-group		Specifies an access group.
name <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. Note This command is not supported in Cisco IOS XE Everest 16.5.1a.
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 <i>cos-value</i> 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...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:

```
Device(config)# class-map class2
Device(config-cmap)# match ip dscp 10 11 12
Device(config-cmap)# exit
```

This example shows how to create a class map called class3, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Device(config)# class-map class3
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# exit
```

This example shows how to delete the IP-precedence match criteria and to classify traffic using acl1:

```
Device(config)# class-map class2
Device(config-cmap)# match ip precedence 5 6 7
Device(config-cmap)# no match ip precedence
Device(config-cmap)# match access-group acl1
Device(config-cmap)# exit
```

This example shows how to specify a list of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

This example shows how to specify a range of physical ports to which an interface-level class map in a hierarchical policy map applies:

```
Device(config)# class-map match-any class4
Device(config-cmap)# match cos 4
Device(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

match non-client-nrt

To match non-client NRT (non-real-time), use the **match non-client-nrt** command in class-map configuration mode. Use the **no** form of this command to return to the default setting.

match non-client-nrt
no match non-client-nrt

Syntax Description	This command has no arguments or keywords.	
Command Default	None	
Command Modes	Class-map	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
Usage Guidelines	None	

This example show how you can configure non-client NRT:

```
Device(config)# class-map test_1000
Device(config-cmap)# match non-client-nrt
```

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 device.

A hierarchical policy map has two levels in the format of a parent-child policy. The parent policy cannot be modified but the child policy (port-child policy) can be modified to suit the QoS configuration.

In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be configured to refer to the VLAN-based policy maps instead of the port-based policy map.



Note Not all MQC QoS combinations are supported for wired ports. For information about these restrictions, see chapters "Restrictions for QoS on Wired 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.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# set dscp 10
Device(config-pmap-c)# police 1000000 20000 conform-action transmit
Device(config-pmap-c)# exit
```

This example show you how to configure hierarchical polices:

```
Switch# configure terminal
Device(config)# class-map c1
Device(config-cmap)# exit

Device(config)# class-map c2
Device(config-cmap)# exit

Device(config)# policy-map child
Device(config-pmap)# class c1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class c2
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# bandwidth 20000
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map parent
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average 1000000
Device(config-pmap-c)# service-policy child
Device(config-pmap-c)# end
```

This example shows how to delete a policy map:

```
Device(config)# no policy-map policymap2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

priority

To assign priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

```
priority [Kbps [burst -in-bytes] ] | level level-value [Kbps [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ]
no priority [Kb/s [burst -in-bytes] ] | level level value [Kb/s [burst -in-bytes] ] | percent
percentage [Kb/s [burst -in-bytes] ] ]
```

Syntax Description		
<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:

```
Device(config)# class-map cm1
Device(config-cmap)#match precedence 2
Device(config-cmap)#exit

Device(config)#class-map cm2
Device(config-cmap)#match dscp 30
Device(config-cmap)#exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)#exit
Device(config-pmap-c)#exit
Device(config-pmap)#exit

Device(config)#policy-map policy1
Device(config-pmap)#class cm2
Device(config-pmap-c)#priority level 2
Device(config-pmap-c)#police 1m
```

queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

queue-buffers ratio *ratio limit*
no queue-buffers ratio *ratio limit*

Syntax Description	<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 queue-buffers ratio 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:

```
Device(config)# policy-map policy_queuebuf01
Device(config-pmap)# class-map class_queuebuf01
Device(config-cmap)# exit
Device(config)# policy policy_queuebuf01
Device(config-pmap)# class class_queuebuf01
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# queue-buffers ratio 10
Device(config-pmap)# end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the **queue-limit** policy-map class configuration command. To remove the queue packet limit from a class, use the **no** form of this command.

```
queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent percentage-of-packets
no queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent
percentage-of-packets
```

Syntax Description

<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:

```
Device(config)# policy-map policy11
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```

service-policy (Wired)

To apply a policy map to a physical port or a switch virtual interface (SVI), use the **service-policy** command in interface configuration mode. Use the **no** form of this command to remove the policy map and port association.

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

Syntax Description

input *policy-map-name* Apply the specified policy map to the input of a physical port or an SVI.

output *policy-map-name* Apply the specified policy map to the output of a physical port or an SVI.

Command Default

No policy maps are attached to the port.

Command Modes

WLAN interface configuration

Command History

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

Usage Guidelines

A policy map is defined by the **policy map** command.

Only one policy map is supported per port, per direction. In other words, only one input policy and one output policy is allowed on any one port.

You can apply a policy map to incoming traffic on a physical port or on an SVI. *QoS Configuration Guide (Catalyst 3850 Switches)*.



Note

Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

Examples

This example shows how to apply plcmap1 to an physical ingress port:

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface gigabitethernet2/0/2
Device(config-if)# no service-policy input plcmap2
```

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS:

```
Device# configure terminal
```

```
Device(config)# class-map vlan100
Device(config-cmap)# match vlan 100
Device(config-cmap)# exit
Device(config)# policy-map vlan100
Device(config-pmap)# policy-map class vlan100
Device(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
Device(config-pmap-c-police)# end
Device# configure terminal
Device(config)# interface gigabitEthernet1/0/5
Device(config-if)# service-policy input vlan100
```

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

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

set cos

{cos-value} | **{cos | dscp | precedence | qos-group}** [**{table table-map-name}**]

set dscp

{dscp-value} | **{cos | dscp | precedence | qos-group}** [**{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}**]

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.

- (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.
- (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.

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:

```
Device(config)# policy-map policy_ftp
Device(config-pmap)# class-map ftp_class
Device(config-cmap)# exit
Device(config)# policy policy_ftp
Device(config-pmap)# class ftp_class
Device(config-pmap-c)# set dscp 10
Device(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

show class-map

To display quality of service (QoS) class maps, which define the match criteria to classify traffic, use the **show class-map** command in EXEC mode.

```
show class-map [class-map-name | type control subscriber {all | class-map-name}]
```

Syntax Description

class-map-name (Optional) Class map name.

type control subscriber (Optional) Displays information about control class maps.

all (Optional) Displays information about all control class maps.

Command Modes

User EXEC

Privileged EXEC

Command History

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

Examples

This is an example of output from the **show class-map** command:

```
Device# show class-map
Class Map match-any videowizard_10-10-10-10 (id 2)
  Match access-group name videowizard_10-10-10-10

Class Map match-any class-default (id 0)
  Match any
Class Map match-any dscp5 (id 3)
  Match ip dscp 5
```

show platform hardware fed switch

To display device-specific hardware information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options, that is, the options available with the **show platform hardware fed switch** *{switch_num | active | standby}* **qos** command.

```
show platform hardware fed switch {switch_num | active | standby} qos {afd | {config type type | [{asic
asic_num}] | stats clients {all | bssid id | wlanid id}} | dscp-cos counters {iifd_id id | interface type number}
| le-info | {iifd_id id | interface type number} | policer config {iifd_id id | interface type number} | queue
| {config | {iifd_id id | interface type number | internal port-type type {asic number [{port_num}]}} |
label2qmap | [{aqmrepqostbl | iqslabtable | sqslabtable}] | {asicnumber} | stats | {iifd_id id | interface
type number | internal {cpu policer | port-type type asic number} {asicnumber [{port_num}]}} | resource}
```

Syntax Description

switch *{switch_num | active | standby}* Switch for which you want to display information. You have the following options:

- *switch_num*—ID of the switch.
- **active**—Displays information relating to the active switch.
- **standby**—Displays information relating to the standby switch, if available.

qos Displays QoS hardware information. You must choose from the following options:

- **afd**—Displays Approximate Fair Drop (AFD) information in hardware.
- **dscp-cos**—Displays information dscp-cos counters for each port.
- **leinfo**—Displays logical entity information.
- **policer**—Displays QoS policer information in hardware.
- **queue**—Displays queue information in hardware.
- **resource**—Displays hardware resource information.

afd *{config type | stats client }* You must choose from the options under **config type** or **stats client** :

config type:

- **client**—Displays wireless client information
- **port**—Displays port-specific information
- **radio**—Displays wireless radio information
- **ssid**—Displays wireless SSID information

stats client :

- **all**—Displays statistics of all client.
- **bssid**—Valid range is from 1 to 4294967295.
- **wlanid**—Valid range is from to 1 4294967295

asicasic_num	(Optional) ASIC number. Valid range is from 0 to 255.
dscp-cos counters { iif_id <i>id</i> interface <i>type number</i> }	Displays per port dscp-cos counters. You must choose from the following options under dscp-cos counters : <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID.
leinfo	You must choose from the following options under dscp-cos counters : <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID.
policer config	Displays configuration information related to policers in hardware. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID.
queue { config { iif_id <i>id</i> interface <i>type</i> <i>number</i> internal } label2qmap stats }	Displays queue information in hardware. You must choose from the following options: <ul style="list-style-type: none"> • config—Configuration information. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID. • internal—Displays internal queue related information. • label2qmap—Displays hardware label to queue mapping information. You can choose from the following options: <ul style="list-style-type: none"> • (Optional) aqmrepqostbl— AQM REP QoS label table lookup. • (Optional) iqslabeltable—IQS QoS label table lookup. • (Optional) sqslabeltable—SQS and local QoS label table lookup. • stats—Displays queue statistics. You must choose from the following options: <ul style="list-style-type: none"> • iif_id <i>id</i>—The target interface ID. Valid range is from 1 to 4294967295. • interface <i>type number</i>—Target interface type and ID. • internal { cpu policer port_type <i>port_type</i> asic <i>asic_num</i> [port_num <i>port_num</i>] }—Displays internal queue related information.
resource	Displays hardware resource usage information. You must enter the following keyword: usage

Command Modes

User EXEC

Privileged EXEC

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

This is an example of output from the `show platform hardware fed switch switch_number qos queue stats internal cpu policer` command

Device#`show platform hardware fed switch 3 qos queue stats internal cpu policer`

QId	PlcIdx	Queue Name	Enabled	Rate		Drop
				(default)	(set)	
0	11	DOT1X Auth	No	1000	1000	0
1	1	L2 Control	No	500	500	0
2	14	Forus traffic	No	1000	1000	0
3	0	ICMP GEN	Yes	200	200	0
4	2	Routing Control	Yes	1800	1800	0
5	14	Forus Address resolution	No	1000	1000	0
6	3	ICMP Redirect	No	500	500	0
7	6	WLESS PRI-5	No	1000	1000	0
8	4	WLESS PRI-1	No	1000	1000	0
9	5	WLESS PRI-2	No	1000	1000	0
10	6	WLESS PRI-3	No	1000	1000	0
11	6	WLESS PRI-4	No	1000	1000	0
12	0	BROADCAST	Yes	200	200	0
13	10	Learning cache ovfl	Yes	100	100	0
14	13	Sw forwarding	Yes	1000	1000	0
15	8	Topology Control	No	13000	13000	0
16	12	Proto Snooping	No	500	500	0
17	16	DHCP Snooping	No	1000	1000	0
18	9	Transit Traffic	Yes	500	500	0
19	10	RPF Failed	Yes	100	100	0
20	15	MCAST END STATION	Yes	2000	2000	0
21	13	LOGGING	Yes	1000	1000	0
22	7	Punt Webauth	No	1000	1000	0
23	10	Crypto Control	Yes	100	100	0
24	10	Exception	Yes	100	100	0
25	3	General Punt	No	500	500	0
26	10	NFL SAMPLED DATA	Yes	100	100	0
27	2	SGT Cache Full	Yes	1800	1800	0
28	10	EGR Exception	Yes	100	100	0
29	16	Show frwd	No	1000	1000	0
30	9	MCAST Data	Yes	500	500	0
31	10	Gold Pkt	Yes	100	100	0

show platform software fed switch qos

To display device-specific software information, use the **show platform hardware fed switch** *switch_number* command.

This topic elaborates only the QoS-specific options available with the **show platform software fed switch** {*switch_num* | **active** | **standby** } **qos** command.

show platform software fed switch{*switch number* | **active** | **standby**}**qos**{**avc** | **internal** | **label2qmap** | **nflqos** | **policer** | **policy** | **qsb** | **tablemap**}

Syntax Description

switch {*switch_num* | **active** | **standby** }
 The device for which you want to display information.

- *switch_num*—Enter the switch ID. Displays information for the specified switch.
- **active**—Displays information for the active switch.
- **standby**—Displays information for the standby switch, if available.

qos
 Displays QoS software information. Choose one the following options:

- **avc** —Displays Application Visibility and Control (AVC) QoS information.
- **internal**—Displays internal queue-related information.
- **label2qmap**—Displays label to queue map table information.
- **nflqos**—Displays NetFlow QoS information.
- **policer**—Displays QoS policer information in hardware.
- **policy**—Displays QoS policy information.
- **qsb**—Displays QoS sub-block information.
- **tablemap**—Displays table mapping information for QoS egress and ingress queues.

Command Modes

User EXEC
 Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

show platform software fed switch qos qsb

To display QoS sub-block information, use the **show platform software fed switch *switch_number* qos qsb** command.

```
show platform software fed switch {switch_number | active | standby} qosqsb {brief | [{all | type |
client_id | port port_number | radio_type | ssidssid}]} | iif_idid | interface |
{Auto-Templateinterface_number | BDIinterface_number | Capwapinterface_number |
GigabitEthernetinterface_number | InternalInterfaceinterface_number | Loopbackinterface_number |
Nullinterface_number | Port-channelinterface_number | TenGigabitEthernetinterface_number |
Tunnelinterface_number | Vlaninterface_number}}
```

Syntax Description

switch { <i>switch_num</i> active standby }	The switch for which you want to display information. <ul style="list-style-type: none"> • <i>switch_num</i>—Enter the ID of the switch. Displays information for the specified switch. • active—Displays information for the active switch. • standby—Displays information for the standby switch, if available.
qos qsb	Displays QoS sub-block software information.

**qsb {brief | iif_id | brief
interface}**

- **all**—Displays information for all client.
- **type**—Displays qsb information for the specified target type:
 - **client**—Displays QoS qsb information for wireless clients
 - **port**—Displays port-specific information
 - **radio**—Displays QoS qsb information for wireless radios
 - **ssid**—Displays QoS qsb information for wireless networks

iif_id—Displays information for the iif_ID

interface—Displays QoS qsb information for the specified interface:

- **Auto-Template**—Auto-template interface between 1 and 999.
- **BDI**—Bridge-domain interface between 1 and 16000.
- **Capwap**—CAPWAP interface between 0 and 2147483647.
- **GigabitEthernet**—GigabitEthernet interface between 0 and 9.
- **InternalInterface**—Internal interface between 0 and 9.
- **Loopback**—Loopback interface between 0 and 2147483647.
- **Null**—Null interface 0-0
- **Port-Channel**—Port-channel interface between 1 and 128.
- **TenGigabitEthernet**—TenGigabitEthernet interface between 0 and 9.
- **Tunnel**—Tunnel interface between 0 and 2147483647.
- **Vlan**—VLAN interface between 1 and 4094.

Command Modes

User EXEC

Privileged EXEC

Command History

Release

Cisco IOS XE Denali 16.1.1

Modification

This command was introduced.

This is an example of the output for the **show platform software fed switch switch_number qos qsb** command

```
Device#sh pl so fed sw 3 qos qsb interface g3/0/2
```

```
QoS subblock information:
Name:GigabitEthernet3/0/2 iif_id:0x0000000000007b iif_type:ETHER(146)
qsb ptr:0xffd8573350
Port type = Wired port
asic_num:0 is_uplink:false init_done:true
FRU events: Active-0, Inactive-0
```



```

def_qos_label:0 def_le_priority:13
trust_enabled:false trust_type:TRUST_DSCP ifm_trust_type:1
LE priority:13 LE trans_index(in, out): (0,0)
Stats (plc,q) export counters (in/out): 0/0
Policy Info:
  Ingress Policy: pmap::{(0xffd8685180,AutoQos-4.0-CiscoPhone-Input-Policy,1083231504,,)}
    tcg::{0xffd867ad10,GigabitEthernet3/0/2 tgt(0x7b,IN) level:0 num_tccg:4 num_child:0},
status:VALID,SET_INHW
  Egress Policy: pmap::{(0xffd86857d0,AutoQos-4.0-Output-Policy,1076629088,,)}
    tcg::{0xffd8685b40,GigabitEthernet3/0/2 tgt(0x7b,OUT) level:0 num_tccg:8 num_child:0},
status:VALID,SET_INHW
  TCG(in,out):(0xffd867ad10, 0xffd8685b40) le_label_id(in,out):(2, 1)
Policer Info:
  num_ag_policers(in,out)[1r2c,2r3c]: ([0,0],[0,0])
  num_mf_policers(in,out): (0,0)
  num_afd_policers:0
  [ag_plc_handle(in,out) = (0xd8688220,0)]
  [mf_plc_handle(in,out)=(nil),(nil)] num_mf_policers:(0,0)
  base:(0xffffffff,0xffffffff) rc:(0,0)]
Queueing Info:
  def_queueing = 0, shape_rate:0 interface_rate_kbps:1000000
  Port shaper:false
  lbl_to_qmap_index:1
Physical qparams:
  Queue Config: NodeType:Physical Id:0x40000049 parent:0x40000049 qid:0 attr:0x1 defq:0

  PARAMS: Excess Ratio:1 Min Cir:1000000 QBuffer:0
  Queue Limit Type:Single Unit:Percent Queue Limit:44192
  SHARED Queue

```

show 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
```

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.

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.

This is an example of the output for the **show policy-map interface** command.

```
Device# show policy-map interface gigabitethernet1/0/48GigabitEthernet1/0/48

Service-policy output: port_shape_parent

Class-map: class-default (match-any)
 191509734 packets
 Match: any
 Queueing

(total drops) 524940551420
(bytes output) 14937264500
```

```
shape (average) cir 250000000, bc 2500000, be 2500000
target shape rate 250000000

Service-policy : child_trip_play

  queue stats for all priority classes:
    Queueing
    priority level 1

    (total drops) 524940551420
    (bytes output) 14937180648

  queue stats for all priority classes:
    Queueing
    priority level 2

    (total drops) 0
    (bytes output) 0

Class-map: dscp56 (match-any)
  191508445 packets
  Match:  dscp cs7 (56)
    0 packets, 0 bytes
    5 minute rate 0 bps
  Priority: Strict,

Priority Level: 1
police:
  cir 10 %
  cir 25000000 bps, bc 781250 bytes
  conformed 0 bytes; actions: >>>>counters not supported
  transmit
  exceeded 0 bytes; actions:
  drop
  conformed 0000 bps, exceeded 0000 bps >>>>counters not supported
```

trust device

To configure trust for supported devices connected to an interface, use the **trust device** command in interface configuration mode. Use the **no** form of this command to disable trust for the connected device.

```
trust device {cisco-phone | cts | ip-camera | media-player}
no trust device {cisco-phone | cts | ip-camera | media-player}
```

Syntax Description	
cisco-phone	Configures a Cisco IP phone
cts	Configures a Cisco TelePresence System
ip-camera	Configures an IP Video Surveillance Camera (IPVSC)
media-player	Configures a Cisco Digital Media Player (DMP)

Command Default Trust disabled

Command Modes Interface configuration

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

Usage Guidelines Use the **trust device** command on the following types of interfaces:

- **Auto**— auto-template interface
- **Capwap**—CAPWAP tunnel interface
- **GigabitEthernet**—Gigabit Ethernet IEEE 802
- **GroupVI**—Group virtual interface
- **Internal Interface**—Internal interface
- **Loopback**—Loopback interface
- **Null**—Null interface
- **Port-channel**—Ethernet Channel interface
- **TenGigabitEthernet**—10-Gigabit Ethernet
- **Tunnel**—Tunnel interface
- **Vlan**—Catalyst VLANs
- **range**—**interface range** command

Example

The following example configures trust for a Cisco IP phone in Interface GigabitEthernet 1/0/1:

```
Device(config)# interface GigabitEthernet1/0/1  
Device(config-if)# trust device cisco-phone
```

You can verify your settings by entering the **show interface status** privileged EXEC command.



PART **XI**

Routing

- [Bidirectional Forwarding Detection, on page 649](#)



Bidirectional Forwarding Detection

- [authentication \(BFD\), on page 650](#)
- [bfd, on page 651](#)
- [bfd all-interfaces, on page 653](#)
- [bfd check-ctrl-plane-failure, on page 654](#)
- [bfd echo, on page 655](#)
- [bfd slow-timers, on page 657](#)
- [bfd template, on page 659](#)
- [bfd-template, on page 660](#)
- [ip route static bfd, on page 661](#)
- [ipv6 route static bfd, on page 663](#)

authentication (BFD)

To configure authentication in a Bidirectional Forwarding Detection (BFD) template for single hop sessions, use the **authentication** command in BFD configuration mode. To disable authentication in BFD template for single-hop sessions, use the **no** form of this command

authentication *authentication-type* **keychain** *keychain-name*
no authentication *authentication-type* **keychain** *keychain-name*

Syntax Description	<i>authentication-type</i>	Authentication type. Valid values are md5, meticulous-md5, meticulous-sha1, and sha-1.
	keychain <i>keychain-name</i>	Configures an authentication key chain with the specified name. The maximum number of characters allowed in the name is 32.

Command Default Authentication in BFD template for single hop sessions is not enabled.

Command Modes BFD configuration (config-bfd)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines You can configure authentication in single hop templates. We recommend that you configure authentication to enhance security. Authentication must be configured on each BFD source-destination pair, and authentication parameters must match on both devices.

Examples

The following example shows how to configure authentication for the template1 BFD single-hop template:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop template1
Device(config-bfd)# authentication sha-1 keychain bfd-singlehop
```

bfd

To set the baseline Bidirectional Forwarding Detection (BFD) session parameters on an interface, use the **bfd** interface configuration mode. To remove the baseline BFD session parameters, use the **no** form of this command

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

Syntax Description	Parameter	Description
	interval <i>milliseconds</i>	Specifies the rate, in milliseconds, at which BFD control packets will be sent to BFD peers. The valid range for the milliseconds argument is from 50 to 9999.
	min_rx <i>milliseconds</i>	Specifies the rate, in milliseconds, at which BFD control packets will be expected to be received from BFD peers. The valid range for the milliseconds argument is from 50 to 9999.
	multiplier <i>multiplier-value</i>	Specifies the number of consecutive BFD control packets that must be missed from a BFD peer before BFD declares that the peer is unavailable and the Layer 3 BFD peer is informed of the failure. The valid range for the multiplier-value argument is from 3 to 50.

Command Default No baseline BFD session parameters are set.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The **bfd** command can be configured on SVI, Ethernet and port-channel interfaces. If BFD runs on a port channel interface, BFD has a timer value restriction of 250 * 3 milliseconds.

The **bfd interval** configuration is not removed when:

- an IPv4 address is removed from an interface
- an IPv6 address is removed from an interface
- IPv6 is disabled from an interface
- an interface is shutdown
- IPv4 CEF is disabled globally or locally on an interface
- IPv6 CEF is disabled globally or locally on an interface

The **bfd interval** configuration is removed when the subinterface on which its is configured is removed.



Note If we configure `bfd interval` command in interface config mode, then `bfd echo` mode is enabled by default. We need to enable either `no ip redirect` (if BFD echo is needed) or `no bfd echo` in interface config mode.

Before using BFD echo mode, you must disable sending Internet Control Message Protocol (ICMP) redirect messages by entering the `no ip redirect` command, in order to avoid high CPU utilization.

Examples

The following example shows the BFD session parameters set for Gigabit Ethernet 1/0/3:

```
Device> enable
Device# configuration terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

bfd all-interfaces

To enable Bidirectional Forwarding Detection (BFD) for all interfaces participating in the routing process, use the **bfd all-interfaces** command in router configuration or address family interface configuration mode. To disable BFD for all neighbors on a single interface, use the **no** form of this command

bfd all-interfaces
no bfd all-interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

BFD is disabled on the interfaces participating in the routing process.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

To enable BFD for all interfaces, enter the **bfd all-interfaces** command in router configuration mode

Examples

The following example shows how to enable BFD for all Enhanced Interior Gateway Routing Protocol (EIGRP) neighbors:

```
Device> enable
Device# configuration terminal
Device(config)# router eigrp 123
Device(config-router)# bfd all-interfaces
Device(config-router)# end
```

The following example shows how to enable BFD for all Intermediate System-to-Intermediate System (IS-IS) neighbors:

```
Device> enable
Device# configuration terminal
Device(config)# router isis tag1
Device(config-router)# bfd all-interfaces
Device(config-router)# end
```

bfd check-ctrl-plane-failure

To enable Bidirectional Forwarding Detection (BFD) control plane failure checking for the Intermediate System-to-Intermediate System (IS-IS) routing protocol, use the **bfd check-control-plane-failure** command in router configuration mode. To disable control plane failure detection, use the **no** form of this command

bfd check-ctrl-plane-failure
no bfd check-ctrl-plane-failure

Syntax Description This command has no arguments or keywords.

Command Default BFD control plane failure checking is disabled.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The **bfd check-ctrl-plane-failure** command can be configured for an IS-IS routing process only. The command is not supported on other protocols.

When a switch restarts, a false BFD session failure can occur, where neighboring routers behave as if a true forwarding failure has occurred. However, if the **bfd check-ctrl-plane-failure** command is enabled on a switch, the router can ignore control plane related BFD session failures. We recommend that you add this command to the configuration of all neighboring routers just prior to a planned router restart, and that you remove the command from all neighboring routers when the restart is complete.

Examples


The following example enables BFD control plane failure checking for the IS-IS routing protocol:

```
Device> enable
Device# configuration terminal
Device(config)# router isis
Device(config-router)# bfd check-ctrl-plane-failure
Device(config-router)# end
```

bfd echo

To enable Bidirectional Forwarding Detection (BFD) echo mode, use the **bfd echo** command in interface configuration mode. To disable BFD echo mode, use the **no** form of this command

bfd echo
no bfd echo

Syntax Description	This command has no arguments or keywords.				
Command Default	BFD echo mode is enabled by default if BFD is configured using bfd interval command in interface configuration mode.				
Command Modes	Interface configuration (config-if)				
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.				
Usage Guidelines	<p>Echo mode is enabled by default. Entering the no bfd echo command without any keywords turns off the sending of echo packets and signifies that the switch is unwilling to forward echo packets received from BFD neighbor switches.</p> <p>When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are taken from the bfd interval <i>milliseconds</i> min_rx <i>milliseconds</i> parameters, respectively.</p>				
 Note	Before using BFD echo mode, you must disable sending Internet Control Message Protocol (ICMP) redirect messages by entering the no ip redirects command, in order to avoid high CPU utilization.				

Examples

The following example configures echo mode between BFD neighbors:

```
Device> enable
Device# configuration terminal
Device(config)# interface GigabitEthernet 1/0/3
Device(config-if)# bfd echo
```

The following output from the **show bfd neighbors details** command shows that the BFD session neighbor is up and using BFD echo mode. The relevant command output is shown in bold in the output.

```
Device# show bfd neighbors details
OurAddr      NeighAddr  LD/RD  RH/RS  Holdown(mult)  State Int
172.16.1.2   172.16.1.1  1/6    Up     0 (3 )         Up   Fa0/1
Session state is UP and using echo function with 100 ms interval.
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 1000000, MinRxInt: 1000000, Multiplier: 3
Received MinRxInt: 1000000, Received Multiplier: 3
Holdown (hits): 3000(0), Hello (hits): 1000(337)
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago
Registered protocols: EIGRP
```

```
Uptime: 00:05:00
Last packet: Version: 1          - Diagnostic: 0
                State bit: Up      - Demand bit: 0
                Poll bit: 0        - Final bit: 0
                Multiplier: 3      - Length: 24
                My Discr.: 6       - Your Discr.: 1
                Min tx interval: 1000000 - Min rx interval: 1000000
                Min Echo interval: 50000
```


bfd slow-timers

To configure the Bidirectional Forwarding Detection (BFD) slow timers value, use the **bfd slow-timers** command in interface configuration mode. To change the slow timers used by BFD, use the **no** form of this command

```
bfd slow-timers [milliseconds]  
no bfd slow-timers
```

Command Default The BFD slow timer value is 1000 milliseconds

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following example shows how to configure the BFD slow timers value to 14,000 milliseconds:

```
Device(config)# bfd slow-timers 14000
```

The following output from the show bfd neighbors details command shows that the BFD slow timers value of 14,000 milliseconds has been implemented. The values for the MinTxInt and MinRxInt will correspond to the configured value for the BFD slow timers. The relevant command output is shown in bold.

```
Device# show bfd neighbors details  
OurAddr      NeighAddr  LD/RD  RH/RS  Holdown(mult)  State  Int  
172.16.1.2   172.16.1.1  1/6    Up      0 (3 )         Up     Fa0/1  
Session state is UP and using echo function with 100 ms interval.  
Local Diag: 0, Demand mode: 0, Poll bit: 0  
MinTxInt: 14000, MinRxInt: 14000, Multiplier: 3  
Received MinRxInt: 1000000, Received Multiplier: 3  
Holdown (hits): 3600(0), Hello (hits): 1200(337)  
Rx Count: 341, Rx Interval (ms) min/max/avg: 1/1008/882 last: 364 ms ago  
Tx Count: 339, Tx Interval (ms) min/max/avg: 1/1016/886 last: 632 ms ago  
Registered protocols: EIGRP  
Uptime: 00:05:00  
Last packet: Version: 1                - Diagnostic: 0  
              State bit: Up            - Demand bit: 0  
              Poll bit: 0              - Final bit: 0  
              Multiplier: 3            - Length: 24  
              My Discr.: 6             - Your Discr.: 1  
              Min tx interval: 1000000 - Min rx interval: 1000000  
              Min Echo interval: 50000
```

**Note**

-
- If the BFD session is down, then the BFD control packets will be sent with the slow timer interval.
 - If the BFD session is up, then if echo is enabled, then BFD control packets will be sent in negotiated slow timer interval and echo packets will be sent in negotiated configured BFD interval. If echo is not enabled, then BFD control packets will be sent in negotiated configured interval.
-

bfd template

To bind a single hop Bidirectional Forwarding Detection (BFD) template to an interface, use the **bfd template** command in interface configuration mode. To unbind single-hop BFD template from an interface, use the **no** form of this command

bfd template *template-name*
no bfd template *template-name*

Command Default A BFD template is not bound to an interface.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Even if you have not created the template by using the **bfd-template** command, you can configure the name of the template under an interface, but the template is considered invalid until you define the template. You do not have to reconfigure the template name again. It becomes valid automatically.

Examples

```
Device> enable
Device# configuration terminal
Device(config)# interface GigabitEthernet 1/3/0
Device(config-if)# bfd template template1
```

bfd-template

To create a Bidirectional Forwarding Detection (BFD) template and to enter BFD configuration mode, use the **bfd-template** command in global configuration mode. To remove a BFD template, use the **no** form of this command

```
bfd-template single-hop template-name
no bfd-template single-hop template-name
```

Syntax Description	single-hop Creates the single-hop BFD template.
	<i>template-name</i> Template name.

Command Default	A BFD template does not exist.
------------------------	--------------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	The bfd-template command allows you to create a BFD template and places the device in BFD configuration mode. The template can be used to specify a set of BFD interval values. BFD interval values specified as part of the BFD template are not specific to a single interface.
-------------------------	--

Examples	The following example shows how to create a BFD template and specify BFD interval values:
-----------------	---

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop node1
Device(bfd-config)#interval min-tx 100 min-rx 100 multiplier 3
Device(bfd-config)#echo
```

The following example shows how to create a BFD single-hop template and configure BFD interval values and an authentication key chain:

```
Device> enable
Device# configuration terminal
Device(config)# bfd-template single-hop template1
Device(bfd-config)#interval min-tx 200 min-rx 200 multiplier 3
Device(bfd-config)#authentication keyed-sha-1 keychain bfd_singlehop
```



Note	BFD echo is not enabled by default in the bfd-template configuration. This needs to be configured explicitly.
-------------	--

ip route static bfd

To specify static route bidirectional forwarding detection (BFD) neighbors, use the **ip route static bfd** command in global configuration mode. To remove a static route BFD neighbor, use the **no** form of this command

```
ip route static bfd { interface-type interface-number ip-address | vrf vrf-name } [group group-name]
[passive] [unassociate]
no ip route static bfd { interface-type interface-number ip-address | vrf vrf-name } [group group-name]
[passive] [unassociate]
```

Syntax Description		
	<i>interface-type interface-number</i>	Interface type and number.
	<i>ip-address</i>	IP address of the gateway, in A.B.C.D format.
	vrf <i>vrf-name</i>	Specifies Virtual Routing and Forwarding (VRF) instance and the destination vrf name.
	group <i>group-name</i>	(Optional) Assigns a BFD group. The group-name is a character string of up to 32 characters specifying the BFD group name.
	unassociate	(Optional) Unassociates the static route configured for a BFD.

Command Default No static route BFD neighbors are specified.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the **ip route static bfd** command to specify static route BFD neighbors. All static routes that have the same interface and gateway specified in the configuration share the same BFD session for reachability notification.

All static routes that specify the same values for the *interface-type*, *interface-number*, and *ip-address* arguments will automatically use BFD to determine gateway reachability and take advantage of fast failure detection.

The **group** keyword assigns a BFD group. The static BFD configuration is added to the VPN routing and forwarding (VRF) instance with which the interface is associated. The **passive** keyword specifies the passive member of the group. Adding static BFD in a group without the **passive** keyword makes the BFD an active member of the group. A static route should be tracked by the active BFD configuration in order to trigger a BFD session for the group. To remove all the static BFD configurations (active and passive) of a specific group, use the **no ip route static bfd** command and specify the BFD group name.

The **unassociate** keyword specifies that a BFD neighbor is not associated with static route, and the BFD sessions are requested if an interface has been configured with BFD. This is useful in bringing up a BFDv4

session in the absence of an IPv4 static route. If the unassociate keyword is not provided, then the IPv4 static routes are associated with BFD sessions.

BFD requires that BFD sessions are initiated on both endpoint devices. Therefore, this command must be configured on each endpoint device.

The BFD static session on a switch virtual interface (SVI) is established only after the **bfd interval milliseconds min_rx milliseconds multiplier multiplier-value** command is disabled and enabled on that SVI.

To enable the static BFD sessions, perform the following steps:

1. Enable BFD timers on the SVI.

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

2. Enable BFD for the static IP route

```
ip route static bfd interface-type interface-number ip-address
```

3. Disable and enable the BFD timers on the SVI again.

```
no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

Examples

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and active member of the group:

```
Device# configuration terminal  
Device(config)# ip route static bfd GigabitEthernet 1/0/1 10.1.1.1 group group1
```

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and passive member of the group:

```
Device# configuration terminal  
Device(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 group group1 passive
```

The following example shows how to configure BFD for all static routes in an unassociated mode without the group and passive keywords:

```
Device# configuration terminal  
Device(config)# ip route static bfd GigabitEthernet 1/0/1 10.2.2.2 unassociate
```

ipv6 route static bfd

To specify static route Bidirectional Forwarding Detection for IPv6 (BFDv6) neighbors, use the **ipv6 route static bfd** command in global configuration mode. To remove a static route BFDv6 neighbor, use the **no** form of this command

ipv6 route static bfd [*vrf vrf-name*] *interface-type interface-number ipv6-address* [**unassociated**]
no ipv6 route static bfd

Syntax Description		
	<i>vrf vrf-name</i>	(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.
	<i>interface-type interface-number</i>	Interface type and number.
	<i>ipv6-address</i>	IPv6 address of the neighbor.
	unassociated	(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.

Command Default No static route BFDv6 neighbors are specified.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the `ipv6 route static bfd` command to specify static route neighbors. All of the static routes that have the same interface and gateway specified in the configuration share the same BFDv6 session for reachability notification. BFDv6 requires that BFDv6 sessions are initiated on both endpoint routers. Therefore, this command must be configured on each endpoint router. An IPv6 static BFDv6 neighbor must be fully specified (with the interface and the neighbor address) and must be directly attached.

All static routes that specify the same values for `vrf vrf-name`, `interface-type interface-number`, and `ipv6-address` will automatically use BFDv6 to determine gateway reachability and take advantage of fast failure detection.

Examples

The following example creates a neighbor on Ethernet interface 0/0 with an address of 2001::1:

```
Device# configuration terminal
Device(config)# ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Device# configuration terminal
Device(config)# ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```




PART **XII**

Security

- [Security](#), on page 667



Security

- [aaa accounting, on page 670](#)
- [aaa accounting dot1x, on page 673](#)
- [aaa accounting identity, on page 675](#)
- [aaa authentication dot1x, on page 677](#)
- [aaa authorization, on page 678](#)
- [aaa authorization network, on page 682](#)
- [aaa new-model, on page 683](#)
- [aaa policy interface-config allow-subinterface, on page 685](#)
- [access-session mac-move deny, on page 686](#)
- [access-session template monitor, on page 688](#)
- [action, on page 689](#)
- [authentication host-mode, on page 690](#)
- [authentication mac-move permit, on page 692](#)
- [authentication priority, on page 694](#)
- [authentication violation, on page 697](#)
- [cisp enable, on page 699](#)
- [clear errdisable interface vlan, on page 700](#)
- [clear mac address-table, on page 701](#)
- [cts manual, on page 703](#)
- [cts role-based enforcement, on page 704](#)
- [cts role-based l2-vrf, on page 706](#)
- [cts role-based monitor, on page 708](#)
- [cts role-based permissions, on page 709](#)
- [deny \(MAC access-list configuration\), on page 710](#)
- [device-role \(IPv6 snooping\), on page 714](#)
- [device-role \(IPv6 nd inspection\), on page 715](#)
- [device-tracking policy, on page 716](#)
- [dot1x critical \(global configuration\), on page 718](#)
- [dot1x max-start, on page 719](#)
- [dot1x pae, on page 720](#)
- [dot1x supplicant controlled transient, on page 721](#)
- [dot1x supplicant force-multicast, on page 722](#)
- [dot1x test eapol-capable, on page 723](#)

- dot1x test timeout, on page 724
- dot1x timeout, on page 725
- epm access-control open, on page 727
- ip access-list role-based, on page 728
- ip admission, on page 729
- ip admission name, on page 730
- ip device tracking maximum, on page 732
- ip device tracking probe, on page 733
- ip dhcp snooping database, on page 734
- ip dhcp snooping information option format remote-id, on page 736
- ip dhcp snooping verify no-relay-agent-address, on page 737
- ip http access-class, on page 738
- ip radius source-interface, on page 740
- ip source binding, on page 742
- ip verify source, on page 743
- ipv6 access-list, on page 744
- ipv6 snooping policy, on page 746
- key chain macsec, on page 747
- limit address-count, on page 748
- mab request format attribute 32, on page 749
- macsec network-link, on page 751
- match (access-map configuration), on page 752
- mka policy (global configuration), on page 754
- mka pre-shared-key, on page 756
- no authentication logging verbose, on page 757
- no dot1x logging verbose, on page 758
- no mab logging verbose, on page 759
- permit (MAC access-list configuration), on page 760
- propagate sgt (cts manual), on page 764
- protocol (IPv6 snooping), on page 766
- radius server, on page 767
- sap mode-list (cts manual), on page 769
- security level (IPv6 snooping), on page 771
- security passthru, on page 772
- server-private (RADIUS), on page 773
- show aaa clients, on page 775
- show aaa command handler, on page 776
- **show aaa local**, on page 777
- show aaa servers, on page 778
- show aaa sessions, on page 779
- show authentication history, on page 780
- show authentication sessions, on page 781
- show cts interface, on page 784
- show cts role-based permissions, on page 786
- show cisp, on page 788
- show dot1x, on page 790

- [show eap pac peer](#), on page 792
- [show ip dhcp snooping statistics](#), on page 793
- [show macsec](#), on page 796
- [show mka policy](#), on page 798
- [show mka session](#), on page 801
- [show mka statistics](#), on page 804
- [show mka summary](#), on page 807
- [show radius server-group](#), on page 810
- [show storm-control](#), on page 812
- [show vlan access-map](#), on page 814
- [show vlan filter](#), on page 815
- [show vlan group](#), on page 816
- [storm-control](#), on page 817
- [switchport port-security aging](#), on page 820
- [switchport port-security mac-address](#), on page 822
- [switchport port-security maximum](#), on page 824
- [switchport port-security violation](#), on page 826
- [tacacs server](#), on page 828
- [tracking \(IPv6 snooping\)](#), on page 829
- [trusted-port](#), on page 831
- [vlan access-map](#), on page 832
- [vlan filter](#), on page 834
- [vlan group](#), on page 835

aaa accounting

To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the **aaa accounting** command in global configuration mode. To disable AAA accounting, use the **no** form of this command.

```
aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
no aaa accounting {auth-proxy | system | network | exec | connections | commands level}
{default | list-name} {start-stop | stop-only | none} [broadcast] group group-name
```

Syntax Description

auth-proxy	Provides information about all authenticated-proxy user events.
system	Performs accounting for all system-level events not associated with users, such as reloads.
network	Runs accounting for all network-related service requests.
exec	Runs accounting for EXEC shell session. This keyword might return user profile information such as what is generated by the autocommand command.
connection	Provides information about all outbound connections made from the network access server.
commands level	Runs accounting for all commands at the specified privilege level. Valid privilege level entries are integers from 0 through 15.
default	Uses the listed accounting methods that follow this argument as the default list of methods for accounting services.
<i>list-name</i>	Character string used to name the list of at least one of the accounting methods described in
start-stop	Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server.
stop-only	Sends a "stop" accounting notice at the end of the requested user process.
none	Disables accounting services on this line or interface.
broadcast	(Optional) Enables sending accounting records to multiple AAA servers. Simultaneously sends accounting records to the first server in each group. If the first server is unavailable, fail over occurs using the backup servers defined within that group.
<i>group groupname</i>	At least one of the keywords described in Table 36: AAA accounting Methods, on page 671

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

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

Usage Guidelines Use the **aaa accounting** command to enable accounting and to create named method lists defining specific accounting methods on a per-line or per-interface basis.

Table 36: AAA accounting Methods

Keyword	Description
group radius	Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.
group tacacs+	Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.
group group-name	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.

In [Table 36: AAA accounting Methods, on page 671](#), the **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** and **aaa group server tacacs+** commands to create a named group of servers.

Cisco IOS software supports the following two methods of accounting:

- **RADIUS**—The network access server reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.
- **TACACS+**—The network access server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server.

Method lists for accounting define the way accounting will be performed. Named accounting method lists enable you to designate a particular security protocol to be used on specific lines or interfaces for particular types of accounting services. Create a list by entering the *list-name* and the *method*, where *list-name* is any character string used to name this list (excluding the names of methods, such as radius or tacacs+) and *method* identifies the methods to be tried in sequence as given.

If the **aaa accounting** command for a particular accounting type is issued without a named method list specified, the default method list is automatically applied to all interfaces or lines (where this accounting type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no accounting takes place.



Note System accounting does not use named accounting lists; you can only define the default list for system accounting.

For minimal accounting, include the **stop-only** keyword to send a stop record accounting notice at the end of the requested user process. For more accounting, you can include the **start-stop** keyword, so that RADIUS

or TACACS+ sends a start accounting notice at the beginning of the requested process and a stop accounting notice at the end of the process. Accounting is stored only on the RADIUS or TACACS+ server. The none keyword disables accounting services for the specified line or interface.

When AAA accounting is activated, the network access server monitors either RADIUS accounting attributes or TACACS+ AV pairs pertinent to the connection, depending on the security method you have implemented. The network access server reports these attributes as accounting records, which are then stored in an accounting log on the security server. For a list of supported RADIUS accounting attributes, refer to the appendix RADIUS Attributes in the *Cisco IOS Security Configuration Guide*. For a list of supported TACACS+ accounting AV pairs, refer to the appendix TACACS+ Attribute-Value Pairs in the *Cisco IOS Security Configuration Guide*.



Note This command cannot be used with TACACS or extended TACACS.

This example defines a default commands accounting method list, where accounting services are provided by a TACACS+ security server, set for privilege level 15 commands with a stop-only restriction:

```
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
```

This example defines a default auth-proxy accounting method list, where accounting services are provided by a TACACS+ security server with a stop-only restriction. The aaa accounting commands activates authentication proxy accounting.

```
Device(config)# aaa new model
Device(config)# aaa authentication login default group TACACS+
Device(config)# aaa authorization auth-proxy default group TACACS+
Device(config)# aaa accounting auth-proxy default start-stop group TACACS+
```


aaa accounting dot1x

To enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions, use the **aaa accounting dot1x** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting dot1x {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+} ... ]}
no aaa accounting dot1x {name | default}
```

Syntax Description

name Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords.

default Specifies the accounting methods that follow as the default list for accounting services.

start-stop Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting notice was received by the accounting server.

broadcast Enables accounting records to be sent to multiple AAA servers and sends accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.

group Specifies the server group to be used for accounting services. These are valid server group names:

- **name** — Name of a server group.
- **radius** — Lists of all RADIUS hosts.
- **tacacs+** — Lists of all TACACS+ hosts.

The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword.

radius (Optional) Enables RADIUS accounting.

tacacs+ (Optional) Enables TACACS+ accounting.

Command Default

AAA accounting is disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command requires access to a RADIUS server.

We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

This example shows how to configure IEEE 802.1x accounting:

```
Device(config)# aaa new-model  
Device(config)# aaa accounting dot1x default start-stop group radius
```

aaa accounting identity

To enable authentication, authorization, and accounting (AAA) accounting for IEEE 802.1x, MAC authentication bypass (MAB), and web authentication sessions, use the **aaa accounting identity** command in global configuration mode. To disable IEEE 802.1x accounting, use the **no** form of this command.

```
aaa accounting identity {name | default} start-stop {broadcast group {name | radius | tacacs+}
[group {name | radius | tacacs+} ... ] | group {name | radius | tacacs+} [group
{name | radius | tacacs+} ... ]}
no aaa accounting identity {name | default}
```

Syntax Description

name	Name of a server group. This is optional when you enter it after the broadcast group and group keywords.
default	Uses the accounting methods that follow as the default list for accounting services.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server.
broadcast	Enables accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server.
group	Specifies the server group to be used for accounting services. These are valid server group names: <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:

```
Device# authentication display new-style
```

Please note that while you can revert to legacy style configuration at any time unless you have explicitly entered new-style configuration, the following caveats should be carefully read and understood.

- (1) If you save the config in this mode, it will be written to NVRAM in NEW-style config, and if you subsequently reload the router without reverting to legacy config and saving that, you will no longer be able to revert.
- (2) In this and legacy mode, Webauth is not IPv6-capable. It will only become IPv6-capable once you have entered new-style config manually, or have reloaded with config saved in 'authentication display new' mode.

```
Device# configure terminal
```

```
Device(config)# aaa accounting identity default start-stop group radius
```

aaa authentication dot1x

To specify the authentication, authorization, and accounting (AAA) method to use on ports complying with the IEEE 802.1x authentication, use the **aaa authentication dot1x** command in global configuration mode on the switch stack or on a standalone switch. To disable authentication, use the **no** form of this command.

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

Syntax Description	default	The default method when a user logs in. Use the listed authentication method that follows this argument.
	<i>method1</i>	Specifies the server authentication. Enter the group radius keywords to use the list of all RADIUS servers for authentication.
	Note	Though other keywords are visible in the command-line help strings, only the default and group radius keywords are supported.
Command Default	No authentication is performed.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **method** argument identifies the method that the authentication algorithm tries in the specified sequence to validate the password provided by the client. The only method that is IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
```

aaa authorization

To set the parameters that restrict user access to a network, use the **aaa authorization** command in global configuration mode. To remove the parameters, use the **no** form of this command.

```
aaa authorization { auth-proxy | cache | commands level | config-commands | configuration
| console | credential-download | exec | multicast | network | onep | policy-if | prepaid
| radius-proxy | reverse-access | subscriber-service | template } { default | list_name }
[method1 [ method2 . . . ]]
```

```
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).
onep	Runs authorization for the ONEP service.
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.

method1 [*method2...*] (Optional) An authorization method or multiple authorization methods to be used for authorization. A method may be any one of the keywords listed in the table below.

Command Default Authorization is disabled for all actions (equivalent to the method keyword **none**).

Command Modes Global configuration

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

Usage Guidelines Use the **aaa authorization** command to enable authorization and to create named methods lists, which define authorization methods that can be used when a user accesses the specified function. Method lists for authorization define the ways in which authorization will be performed and the sequence in which these methods will be performed. A method list is a named list that describes the authorization methods (such as RADIUS or TACACS+) that must be used in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, which ensures a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or until all the defined methods are exhausted.



Note The Cisco IOS software attempts authorization with the next listed method only when there is no response from the previous method. If authorization fails at any point in this cycle--meaning that the security server or the local username database responds by denying the user services--the authorization process stops and no other authorization methods are attempted.

If the **aaa authorization** command for a particular authorization type is issued without a specified named method list, the default method list is automatically applied to all interfaces or lines (where this authorization type applies) except those that have a named method list explicitly defined. (A defined method list overrides the default method list.) If no default method list is defined, then no authorization takes place. The default authorization method list must be used to perform outbound authorization, such as authorizing the download of IP pools from the RADIUS server.

Use the **aaa authorization** command to create a list by entering the values for the *list-name* and the *method* arguments, where *list-name* is any character string used to name this list (excluding all method names) and *method* identifies the list of authorization methods tried in the given sequence.



Note In the table that follows, the **group***group-name*, **group ldap**, **group radius**, and **group tacacs+** methods refer to a set of previously defined RADIUS or TACACS+ servers. Use the **radius server** 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 37: aaa authorization Methods

Keyword	Description
cache <i>group-name</i>	Uses a cache server group for authorization.
group <i>group-name</i>	Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name command.
group ldap	Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.
group radius	Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.
grouptacacs+	Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.
if-authenticated	Allows the user to access the requested function if the user is authenticated. Note The if-authenticated method is a terminating method. Therefore, if it is listed as a method, any methods listed after it will never be evaluated.
local	Uses the local database for authorization.
none	Indicates that no authorization is performed.

Cisco IOS software supports the following methods for authorization:

- Cache Server Groups—The router consults its cache server groups to authorize specific rights for users.
- If-Authenticated—The user is allowed to access the requested function provided the user has been authenticated successfully.
- Local—The router or access server consults its local database, as defined by the **username** command, to authorize specific rights for users. Only a limited set of functions can be controlled through the local database.
- None—The network access server does not request authorization information; authorization is not performed over this line or interface.
- RADIUS—The network access server requests authorization information from the RADIUS security server group. RADIUS authorization defines specific rights for users by associating attributes, which are stored in a database on the RADIUS server, with the appropriate user.
- TACACS+—The network access server exchanges authorization information with the TACACS+ security daemon. TACACS+ authorization defines specific rights for users by associating attribute-value (AV) pairs, which are stored in a database on the TACACS+ security server, with the appropriate user.

Method lists are specific to the type of authorization being requested. AAA supports five different types of authorization:

- **Commands**—Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- **EXEC**—Applies to the attributes associated with a user EXEC terminal session.
- **Network**—Applies to network connections. The network connections can include a PPP, SLIP, or ARA connection.



Note You must configure the **aaa authorization config-commands** command to authorize global configuration commands, including EXEC commands prepended by the **do** command.

- **Reverse Access**—Applies to reverse Telnet sessions.
- **Configuration**—Applies to the configuration downloaded from the AAA server.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Once defined, the method lists must be applied to specific lines or interfaces before any of the defined methods are performed.

The authorization command causes a request packet containing a series of AV pairs to be sent to the RADIUS or TACACS daemon as part of the authorization process. The daemon can do one of the following:

- Accept the request as is.
- Make changes to the request.
- Refuse the request and authorization.

For a list of supported RADIUS attributes, see the module RADIUS Attributes. For a list of supported TACACS+ AV pairs, see the module TACACS+ Attribute-Value Pairs.



Note Five commands are associated with privilege level 0: **disable**, **enable**, **exit**, **help**, and **logout**. If you configure AAA authorization for a privilege level greater than 0, these five commands will not be included in the privilege level command set.

The following example shows how to define the network authorization method list named `mygroup`, which specifies that RADIUS authorization will be used on serial lines using PPP. If the RADIUS server fails to respond, local network authorization will be performed.

```
Device(config)# aaa authorization network mygroup group radius local
```

aaa authorization network

To configure the switch to use user-RADIUS authorization for all network-related service requests, such as IEEE 802.1x VLAN assignment, use the **aaa authorization network** command in global configuration mode. To disable RADIUS user authorization, use the **no** form of this command

aaa authorization network default group radius
no aaa authorization network default

Syntax Description	default group radius Use the list of all RADIUS hosts in the server group as the default authorization list.	
Command Default	Authorization is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
Usage Guidelines	Use the aaa authorization network default group radius global configuration command to allow the switch to download IEEE 802.1x authorization parameters from the RADIUS servers in the default authorization list. The authorization parameters are used by features such as VLAN assignment to get parameters from the RADIUS servers.	
	Use the show running-config privileged EXEC command to display the configured lists of authorization methods.	
This example shows how to configure the switch for user RADIUS authorization for all network-related service requests:		
<pre>Device(config)# aaa authorization network default group radius</pre>		

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.

aaa policy interface-config allow-subinterface

To enable authentication, authorization, and accounting (AAA) Link Control Protocol (LCP) interface configuration policy parameters, issue the **aaa policy interface-config allow-subinterface** command in global configuration mode. To disable LCP interface configuration policy parameters, use the **no** form of this command.

```
aaa policy interface-config allow-subinterface
no aaa policy interface-config allow-subinterface
```

Syntax Description

interface-config Specifies the LCP interface configuration policy parameters.

allow-subinterface Specifies not to create a full virtual access interface by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 3.6.0E	This command was introduced.

Usage Guidelines

Use the **interface-config** keyword to apply interface configuration mode commands on the virtual access interface associated with the session.

Examples

The following example shows how to enable AAA LCP interface configuration policy parameters:

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa policy interface-config allow-subinterface
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.

access-session mac-move deny

To disable MAC move on a device, use the **access-session mac-move deny** global configuration command. To return to the default setting, use the **no** form of this command.

access-session mac-move deny
no access-session mac-move deny

Syntax Description This command has no arguments or keywords.

Command Default MAC move is enabled.

Command Modes Global configuration

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

Usage Guidelines The **no** form of this command enables authenticated hosts to move between any authentication-enabled ports (MAC authentication bypass [MAB], 802.1x, or Web-auth) on a device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# no access-session mac-move deny
```

Related Commands	Command	Description
	authentication event	Sets the action for specific authentication events.
	authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	authentication host-mode	Sets the authorization manager mode on a port.
	authentication open	Enables or disables open access on a port.
	authentication order	Sets the order of authentication methods used on a port.
	authentication periodic	Enables or disables reauthentication on a port.
	authentication port-control	Enables manual control of the port authorization state.

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.

access-session template monitor

To set the access session template to monitor ports, use the **access-session template monitor** command in global configuration mode. To return to the default setting, use the **no** form of this command.

access-session template monitor

no access-session template monitor

Syntax Description This command has no arguments or keywords.

Command Default This command is not configured.

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The **access-session template monitor** command enables session monitoring to create sessions on all ports where authentication configurations are not present, and MAC addresses are known. These sessions have open access ports for traffic, multi-auth host mode to control the number of hosts on a port, and port-control set to auto for sessions to undergo authentication and authorization. The **access-session template monitor** command is enabled by default if the **device classifier** or **autoconf** command is enabled. Session monitoring can be disabled on a per port basis.

This command is available on devices that has Identity-Based Networking Services (IBNS). The equivalent command for **access-session template monitor** command in IBNS **new-style** mode is **access-session monitor**. To switch from IBNS legacy mode to new style mode, use the **authentication convert-to new-style** command.

Examples

The following example shows how to set the access session template to monitor ports:

```
Device(config)# access-session template monitor
```

Related Commands

Command	Description
device classifier	Creates a monitor session for all the MAC addresses learned in the system.
authentication convert-to new-style	Converts all the relevant authentication commands to their CPL control policy-equivalents.

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:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address a12
Device(config-access-map)# action forward
Device(config-access-map)# exit
Device(config)# vlan filter vmap4 vlan-list 5-6
```

authentication host-mode

To set the authorization manager mode on a port, use the **authentication host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

authentication host-mode { **multi-auth** | **multi-domain** | **multi-host** | **single-host** }
no authentication host-mode

Syntax Description		
multi-auth		Enables multiple-authorization mode (multi-auth mode) on the port.
multi-domain		Enables multiple-domain mode on the port.
multi-host		Enables multiple-host mode on the port.
single-host		Enables single-host mode on the port.

Command Default Single host mode is enabled.

Command Modes Interface configuration

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

Usage Guidelines Single-host mode should be configured if only one data host is connected. Do not connect a voice device to authenticate on a single-host port. Voice device authorization fails if no voice VLAN is configured on the port.

Multi-domain mode should be configured if data host is connected through an IP phone to the port. Multi-domain mode should be configured if the voice device needs to be authenticated.

Multi-auth mode should be configured to allow devices behind a hub to obtain secured port access through individual authentication. Only one voice device can be authenticated in this mode if a voice VLAN is configured.

Multi-host mode also offers port access for multiple hosts behind a hub, but multi-host mode gives unrestricted port access to the devices after the first user gets authenticated.

This example shows how to enable multi-auth mode on a port:

```
Device(config-if)# authentication host-mode multi-auth
```

This example shows how to enable multi-domain mode on a port:

```
Device(config-if)# authentication host-mode multi-domain
```

This example shows how to enable multi-host mode on a port:

```
Device(config-if) # authentication host-mode multi-host
```

This example shows how to enable single-host mode on a port:

```
Device(config-if) # authentication host-mode single-host
```

You can verify your settings by entering the **show authentication sessions interface *interface* details** privileged EXEC command.

authentication mac-move permit

To enable MAC move on a device, use the **authentication mac-move permit** command in global configuration mode. To disable MAC move, use the **no** form of this command.

authentication mac-move permit
no authentication mac-move permit

Syntax Description This command has no arguments or keywords.

Command Default MAC move is 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 device. For example, if there is a device between an authenticated host and port, and that host moves to another port, the authentication session is deleted from the first port, and the host is reauthenticated on the new port.

If MAC move is disabled, and an authenticated host moves to another port, it is not reauthenticated, and a violation error occurs.

This example shows how to enable MAC move on a device:

```
Device(config)# authentication mac-move permit
```

Related Commands


Command	Description
access-session mac-move deny	Disables MAC move on a device.
authentication event	Sets the action for specific authentication events.
authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
authentication host-mode	Sets the authorization manager mode on a port.
authentication open	Enables or disables open access on a port.
authentication order	Sets the order of authentication methods used on a port.
authentication periodic	Enable or disables reauthentication on a port.

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	<table border="1"> <tr> <td data-bbox="324 535 893 619">dot1x</td> <td data-bbox="893 535 1502 619">(Optional) Adds 802.1x to the order of authentication methods.</td> </tr> <tr> <td data-bbox="324 619 893 703">mab</td> <td data-bbox="893 619 1502 703">(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.</td> </tr> <tr> <td data-bbox="324 703 893 808">webauth</td> <td data-bbox="893 703 1502 808">Adds web authentication to the order of authentication methods.</td> </tr> </table>	dot1x	(Optional) Adds 802.1x to the order of authentication methods.	mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.	webauth	Adds web authentication to the order of authentication methods.
dot1x	(Optional) Adds 802.1x to the order of authentication methods.						
mab	(Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.						
webauth	Adds web authentication to the order of authentication methods.						
Command Default	The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.						
Command Modes	Interface configuration						
Command History	<table border="1"> <thead> <tr> <th data-bbox="324 955 1055 997">Release</th> <th data-bbox="1055 955 1502 997">Modification</th> </tr> </thead> <tbody> <tr> <td data-bbox="324 1018 1055 1081">Cisco IOS XE 3.2SE</td> <td data-bbox="1055 1018 1502 1081">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> <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>Device(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>						

```
Device(config-if) # authentication priority mab webauth
```

Related Commands	Command	Description
	authentication control-direction	Configures the port mode as unidirectional or bidirectional.
	authentication event fail	Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.
	authentication event no-response action	Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.
	authentication event server alive action reinitialize	Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.
	authentication event server dead action authorize	Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.
	authentication fallback	Enables a web authentication fallback method.
	authentication host-mode	Allows hosts to gain access to a controlled port.
	authentication open	Enables open access on a port.
	authentication order	Specifies the order in which the Auth Manager attempts to authenticate a client on a port.
	authentication periodic	Enables automatic reauthentication on a port.
	authentication port-control	Configures the authorization state of a controlled port.
	authentication timer inactivity	Configures the time after which an inactive Auth Manager session is terminated.
	authentication timer reauthenticate	Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.
	authentication timer restart	Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.
	authentication violation	Specifies the action to be taken when a security violation occurs on a port.
	mab	Enables MAC authentication bypass on a port.

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	protect	Drops unexpected incoming MAC addresses. No syslog errors are generated.
	replace	Removes the current session and initiates authentication with the new host.
	restrict	Generates a syslog error when a violation error occurs.
	shutdown	Error-disables the port or the virtual port on which an unexpected MAC address occurs.

Command Default Authentication violation shutdown mode is enabled.

Command Modes Interface configuration

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

Usage Guidelines Use the **authentication violation** command to specify the action to be taken when a security violation occurs on a port.

This example shows how to configure an IEEE 802.1x-enabled port as error-disabled and to shut down when a new device connects it:

```
Device(config-if) # authentication violation shutdown
```

This example shows how to configure an 802.1x-enabled port to generate a system error message and to change the port to restricted mode when a new device connects to it:

```
Device(config-if) # authentication violation restrict
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:

```
Device(config-if) # authentication violation protect
```

This example shows how to configure an 802.1x-enabled port to remove the current session and initiate authentication with a new device when it connects to the port:

```
Device(config-if)# authentication violation replace
```

You can verify your settings by entering the **show authentication** privileged EXEC command.

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:

```
Device(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 reenabling 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 reenabling 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 reenabling all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

Related Commands	Command	Description
	errdisable detect cause	Enables error-disabled detection for a specific cause or all causes.
	errdisable recovery	Configures the recovery mechanism variables.
	show errdisable detect	Displays error-disabled detection status.
	show errdisable recovery	Displays error-disabled recovery timer information.
	show interfaces status err-disabled	Displays interface status of a list of interfaces in error-disabled state.

clear mac address-table

To delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members, or all dynamic addresses on a particular VLAN, use the **clear mac address-table** command in privileged EXEC mode. This command also clears the MAC address notification global counters.

```
clear mac address-table {dynamic [address mac-addr | interface interface-id | vlan vlan-id]
| move update | notification}
```

Syntax Description		
dynamic		Deletes all dynamic MAC addresses.
address <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:

```
Device# clear mac address-table dynamic address 0008.0070.0007
```

Related Commands	Command	Description
	mac address-table notification	Enables the MAC address notification feature.
	mac address-table move update { receive transmit }	Configures MAC address-table move update on the switch.

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.

cts manual

To manually enable an interface for Cisco TrustSec Security (CTS), use the **cts manual** command in interface configuration mode.

cts manual

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines

Use the **cts manual** command to enter the TrustSec manual interface configuration in which policies and the Security Association Protocol (SAP) are configured on the link.

When **cts manual** command is configured, 802.1X authentication is not performed on the link. Use the **policy** subcommand to define and apply policies on the link. By default no policy is applied. To configure MACsec link-to-link encryption, the SAP negotiation parameters must be defined. By default SAP is not enabled. The same SAP Pairwise master key (PMK) should be configured on both sides of the link (that is, a shared secret)

Examples

The following example shows how to enter the Cisco TrustSec manual mode:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)#
```

The following example shows how to remove the CTS manual configuration from an interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# no cts manual
```

Related Commands

Command	Description
propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
sap mode-list (cts manual)	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.
show cts interface	Displays Cisco TrustSec interface configuration statistics.

cts role-based enforcement

To enable Cisco TrustSec role-based (security group) access control enforcement, use the **cts role-based enforcement** command in global configuration mode. To disable the configuration, use the **no** form of this command.

```
cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [{,}] [{-}]}}]
no cts role-based enforcement [{logging-interval interval | vlan-list {all | vlan-ID [{,}] [{-}]}}]
```

Syntax Description

logging-interval <i>interval</i>	(Optional) Configures a logging interval for a security group access control list (SGACL). Valid values for the <i>interval</i> argument are from 5 to 86400 seconds. The default is 300 seconds
vlan-list	(Optional) Configures VLANs on which role-based ACLs are enforced.
all	(Optional) Specifies all VLANs.
<i>vlan-ID</i>	(Optional) VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

Command Default

Role-based access control is not enforced.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines



Note RBACL and SGACL are used interchangeably.

Use the **cts role-based enforcement** command to globally enable or disable SGACL enforcement for Cisco TrustSec-enabled interfaces in the system.

The default interval after which log for a given flow is printed is 300 seconds. Use the **logging-interval** keyword to change the default interval. Logging is only triggered when the Cisco ACE Application Control Engine has the **logging** keyword.

SGACL enforcement is not enabled by default on VLANs. Use the **cts role-based enforcement vlan-list** command to enable or disable SGACL enforcement for Layer 2 switched packets and for Layer 3 switched packets on an switched virtual interface (SVI).

The *vlan-ID* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges.

When a VLAN in which a SGACL is enforced has an active SVI, the SGACL is enforced for both Layer 2 and Layer 3 switched packets within that VLAN. Without an SVI, the SGACL is enforced only for Layer 2 switched packets, because no Layer 3 switching is possible within a VLAN without an SVI.

The following example shows configure an SGACL logging interval:

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit

May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0/2' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

Related Commands

Command	Description
logging rate-limit	Limits the rate of messages logged per second.
show cts role-based permissions	Displays the SGACL permission list.

cts role-based l2-vrf

To select a virtual routing and forwarding (VRF) instance for Layer 2 VLANs, use the **cts role-based l2-vrf** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
no cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
```

Syntax Description

<i>vrf-name</i>	Name of the VRF instance.
vlan-list	Specifies the list of VLANs to be assigned to a VRF instance.
all	Specifies all VLANs.
<i>vlan-ID</i>	VLAN ID. Valid values are from 1 to 4094.
,	(Optional) Specifies another VLAN separated by a comma.
-	(Optional) Specifies a range of VLANs separated by a hyphen.

Command Default

VRF instances are not selected.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

The *vlan-list* argument can be a single VLAN ID, a list of comma-separated VLAN IDs, or hyphen-separated VLAN ID ranges.

The **all** keyword is equivalent to the full range of VLANs supported by the network device. The **all** keyword is not preserved in the nonvolatile generation (NVGEN) process.

If the **cts role-based l2-vrf** command is issued more than once for the same VRF, each successive command entered adds the VLAN IDs to the specified VRF.

The VRF assignments configured by the **cts role-based l2-vrf** command are active as long as a VLAN remains a Layer 2 VLAN. The IP-SGT bindings learned while a VRF assignment is active are also added to the Forwarding Information Base (FIB) table associated with the VRF and the IP protocol version. If an Switched Virtual Interface (SVI) becomes active for a VLAN, the VRF-to-VLAN assignment becomes inactive and all bindings learned on the VLAN are moved to the FIB table associated with the VRF of the SVI.

Use the **interface vlan** command to configure an SVI interface, and the **vrf forwarding** command to associate a VRF instance to the interface.

The VRF-to-VLAN assignment is retained even when the assignment becomes inactive. It is reactivated when the SVI is removed or when the SVI IP address is changed. When reactivated, the IP-SGT bindings are moved back from the FIB table associated with the VRF of the SVI to the FIB table associated with the VRF assigned by the **cts role-based l2-vrf** command.

The following example shows how to select a list of VLANs to be assigned to a VRF instance:

```
Switch(config)# cts role-based l2-vrf vrf1 vlan-list 20
```

The following example shows how to configure an SVI interface and associate a VRF instance:

```
Switch(config)# interface vlan 101  
Switch(config-if)# vrf forwarding vrf1
```

Related Commands

Command	Description
interface vlan	Configures a VLAN interface.
vrf forwarding	Associates a VRF instance or a virtual network with an interface or subinterface.
show cts role-based permissions	Displays the SGACL permission list.

cts role-based monitor

To enable role-based (security-group) access list monitoring, use the **cts role-based monitor** command in global configuration mode. To remove role-based access list monitoring, use the **no** form of this command.

```
cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown}
[{{ipv4}}]}
no cts role-based monitor {all | permissions | {default | from {sgt | unknown}} to {sgt | unknown}
[{{ipv4}}]}
```

Syntax Description

all	Monitors permissions for all source tags to all destination tags.
permissions	Monitors permissions from a source tags to a destination tags.
default	Monitors the default permission list.
from	Specifies the source group tag for filtered traffic.
<i>sgt</i>	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag (DST).
ipv4	(Optional) Specifies the IPv4 protocol.

Command Default

Role-based access control monitoring is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Use the **cts role-based monitor all** command to enable the global monitor mode. If the **cts role-based monitor all** command is configured, the output of the **show cts role-based permissions** command displays monitor mode for all configured policies as true.

The following examples shows how to configure SGACL monitor from a source tag to a destination tag:

```
Switch(config)# cts role-based monitor permissions from 10 to 11
```

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

cts role-based permissions

To enable permissions from a source group to a destination group, use the **cts role-based permissions** command in global configuration mode. To remove the permissions, use the **no** form of this command.

```
cts role-based permissions {default ipv4 | from {sgt | unknown} to {sgt | unknown} {ipv4}
{rbacl-name [{rbacl-name....}]}}
no cts role-based permissions {default [{ipv4}] | from {sgt | unknown} to {sgt
| unknown} [{ipv4}]}
```

Syntax Description

default	Specifies the default permissions list. Every cell (an SGT pair) for which, security group access control list (SGACL) permission is not configured statically or dynamically falls under the default category.
ipv4	Specifies the IPv4 protocol.
from	Specifies the source group tag of the filtered traffic.
<i>sgt</i>	Security Group Tag (SGT). Valid values are from 2 to 65519.
unknown	Specifies an unknown source or destination group tag.
<i>rbacl-name</i>	Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.

Command Default

Permissions from a source group to a destination group is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

Use the **cts role-based permissions** command to define, replace, or delete the list of SGACLs for a given source group tag (SGT), destination group tag (DGT) pair. This policy is in effect as long as there is no dynamic policy for the same DGT or SGT.

The **cts role-based permissions default** command defines, replaces, or deletes the list of SGACLs of the default policy as long as there is no dynamic policy for the same DGT.

The following example shows how to enable permissions for a destination group:

```
Switch(config)# cts role-based permissions from 6 to 6 mon_2
```

Related Commands

Command	Description
show cts role-based permissions	Displays the SGACL permission list.

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.
lavc-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. <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 38: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novel Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with EtherType 0x4321:

```
Device(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.
permit	Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.

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	<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 device-role command specifies the role of the device attached to the port. By default, the device role is node.</p> <p>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.</p> <p>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:</p> <pre>Device(config)# ipv6 snooping policy policy1 Device(config-ipv6-snooping)# device-role node</pre>				

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 | switch }
```

Syntax Description	host	Sets the role of the attached device to host.
	switch	Sets the role of the attached device to switch.
Command Default	The device role is host.	
Command Modes	ND inspection policy configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines

The **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked.

The **switch** keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
```

device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the **device-tracking** command in global configuration mode. To delete a device tracking policy, use the **no** form of this command.

device -tracking policy *policy-name*
no device-tracking policy *policy-name*

Syntax Description	<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:

```
Device(config)# device-tracking policy policy1  
Device(config-device-tracking)# trusted-port
```

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical eapol

Syntax Description	eapol Specifies that the switch send an EAPOL-Success message when the switch successfully authenticates the critical port.				
Command Default	eapol is disabled				
Command Modes	Global configuration				
Command History	<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:

```
Device(config)# dot1x critical eapol
```

dot1x max-start

To set the maximum number of Extensible Authentication Protocol over LAN (EAPOL) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start** command in interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

```
dot1x max-start number
no dot1x max-start
```

Syntax Description

number Maximum number of times that the router sends an EAPOL start frame. The value is from 1 to 10. The default is 3.

Command Default

The default maximum number setting is 3.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

You must enter the **switchport mode access** interface configuration command on a switch port before entering this command.

The following example shows that the maximum number of EAPOL Start requests has been set to 5:

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x max-start 5
```

dot1x 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 | both}
no dot1x pae {supplicant | authenticator | both}
```

Syntax Description

supplicant	The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

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:

```
Device(config)# interface g1/0/3
Device(config-if)# dot1x pae supplicant
```


dot1x supplicant controlled transient

To control access to an 802.1x supplicant port during authentication, use the **dot1x supplicant controlled transient** command in global configuration mode. To open the supplicant port during authentication, use the **no** form of this command

dot1x supplicant controlled transient
no dot1x supplicant controlled transient

Syntax Description

This command has no arguments or keywords.

Command Default

Access is allowed to 802.1x supplicant ports during authentication.

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

In the default state, when you connect a supplicant switch to an authenticator switch that has BPCU guard enabled, the authenticator port could be error-disabled if it receives a Spanning Tree Protocol (STP) bridge protocol data unit (BPDU) packets before the supplicant switch has authenticated. Beginning with Cisco IOS Release 15.0(1)SE, you can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** global configuration command temporarily blocks the supplicant port during authentication to ensure that the authenticator port does not shut down before authentication completes. If authentication fails, the supplicant port opens. Entering the **no dot1x supplicant controlled transient** global configuration command opens the supplicant port during the authentication period. This is the default behavior.

We strongly recommend using the **dot1x supplicant controlled transient** command on a supplicant switch when BPDU guard is enabled on the authenticator switch port with the **spanning-tree bpduguard enable** interface configuration command.

This example shows how to control access to 802.1x supplicant ports on a switch during authentication:

```
Device(config)# dot1x supplicant controlled transient
```

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:

```
Device(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 interface-id (Optional) Port to be queried.				
Command Default	There is no default setting.				
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.				

Usage Guidelines Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a no form of this command.

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
Device# dot1x test eapol-capable interface gigabitethernet1/0/13
```

```
DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable
```

Related Commands	Command	Description
	dot1x test timeout timeout	Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.

dot1x test timeout

To configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness, use the **dot1x test timeout** command in global configuration mode on the switch stack or on a standalone switch.

dot1x test timeout *timeout*

Syntax Description	<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:

```
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

Related Commands	Command	Description
	dot1x test eapol-capable [<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>	<p>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).</p> <p>The range is from 1 to 65535. The default is 30.</p>
held-period <i>seconds</i>	<p>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).</p> <p>The range is from 1 to 65535. The default is 60</p>
quiet-period <i>seconds</i>	<p>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.</p> <p>The range is from 1 to 65535. The default is 60</p>
ratelimit-period <i>seconds</i>	<p>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).</p> <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>	<p>Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.</p> <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>	<p>Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.</p> <p>The range is from 1 to 65535. The default is 30.</p> <p>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.</p>

supp-timeout *seconds* Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID.
The range is from 1 to 65535. The default is 30.

tx-period *seconds* Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client.

- The range is from 1 to 65535. The default is 30.
- If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default Periodic reauthentication and periodic rate-limiting are done.

Command Modes Interface configuration

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

Usage Guidelines You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

When the **ratelimit-period** is set to 0 (the default), the switch does not ignore EAPOL packets from clients that have been successfully authenticated and forwards them to the RADIUS server.

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Device(config)# configure terminal
Device(config)# interface g1/0/3
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x timeout auth-period 2000
Device(config-if)# dot1x timeout held-period 2400
Device(config-if)# dot1x timeout quiet-period 600
Device(config-if)# dot1x timeout start-period 90
Device(config-if)# dot1x timeout supp-timeout 300
Device(config-if)# dot1x timeout tx-period 60
Device(config-if)# dot1x timeout server-timeout 60
```

epm access-control open

To configure an open directive for ports that do not have an access control list (ACL) configured, use the **epm access-control open** command in global configuration mode. To disable the open directive, use the **no** form of this command.

epm access-control open
no epm access-control open

Syntax Description This command has no arguments or keywords.

Command Default The default directive applies.

Command Modes Global configuration

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

Usage Guidelines Use this command to configure an open directive that allows hosts without an authorization policy to access ports configured with a static ACL. If you do not configure this command, the port applies the policies of the configured ACL to the traffic. If no static ACL is configured on a port, both the default and open directives allow access to the port.

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

This example shows how to configure an open directive.

```
Device(config)# epm access-control open
```

Related Commands	Command	Description
	show running-config	Displays the contents of the current running configuration file.

ip access-list role-based

To create a role-based (security group) access control list (RBACL) and enter role-based ACL configuration mode, use the **ip access-list role-based** command in global configuration mode. To remove the configuration, use the **no** form of this command.

```
ip access-list role-based access-list-name
no ip access-list role-based access-list-name
```

Syntax Description	<i>access-list-name</i> Name of the security group access control list (SGACL).
---------------------------	---

Command Default	Role-based ACLs are not configured.
------------------------	-------------------------------------

Command Modes	Global configuration (config)
----------------------	-------------------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines	For SGACL logging, you must configure the permit ip log command. Also, this command must be configured in Cisco Identity Services Engine (ISE) to enable logging for dynamic SGACLs.
-------------------------	---

The following example shows how to define an SGACL that can be applied to IPv4 traffic and enter role-based access list configuration mode:

```
Switch(config)# ip access-list role-based rbac11
Switch(config-rb-acl)# permit ip log
```

Related Commands	Command	Description
	permit ip log	Permits logging that matches the configured entry.
	show ip access-list	Displays contents of all current IP access lists.

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 switchport.

This example shows how to apply a web authentication rule to a switchport:

```
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
```

This example shows how to apply a web authentication rule to a fallback profile for use on an IEEE 802.1x enabled switch port.

```
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
```

ip admission name

To enable web authentication, use the **ip admission name** command in global configuration mode. To disable web authentication, use the **no** form of this command.

ip admission name *name* { **consent** | **proxy http** } [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** { *acl* | *acl-name* } | **service-policy type tag** *service-policy-name*]
no ip admission name *name* { **consent** | **proxy http** } [**absolute timer** *minutes* | **inactivity-time** *minutes* | **list** { *acl* | *acl-name* } | **service-policy type tag** *service-policy-name*]

Syntax Description

<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>polycyname</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:

```
Device# configure terminal
Device(config) ip admission name http-rule proxy http
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 101 in
Device(config-if)# ip admission rule
Device(config-if)# end
```

This example shows how to configure IEEE 802.1x authentication with web authentication as a fallback mechanism on a switch port:

```
Device# configure terminal
Device(config)# ip admission name rule2 proxy http
Device(config)# fallback profile profile1
Device(config)# ip access group 101 in
Device(config)# ip admission name rule2
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# dot1x port-control auto
Device(config-if)# dot1x fallback profile1
Device(config-if)# end
```

Related Commands

Command	Description
dot1x fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
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:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# ip device tracking
Device(config)# interface gigabitethernet1/0/3
Device(config-if)# switchport mode access
Device(config-if)# switchport access vlan 1
Device(config-if)# ip device tracking maximum 5
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
Device(config-if)# end
```

ip device tracking probe

To configure the IP device tracking table for Address Resolution Protocol (ARP) probes, use the **ip device tracking probe** command in global configuration mode. To disable ARP probes, use the **no** form of this command.

```
ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
no ip device tracking probe {count number | delay seconds | interval seconds | use-svi address}
```

Syntax Description	
count <i>number</i>	Sets the number of times that the device sends the ARP probe. The range is from 1 to 255.
delay <i>seconds</i>	Sets the number of seconds that the device waits before sending the ARP probe. The range is from 1 to 120.
interval <i>seconds</i>	Sets the number of seconds that the device waits for a response before resending the ARP probe. The range is from 30 to 1814400 seconds.
use-svi	Uses the switch virtual interface (SVI) IP address as source of ARP probes.

Command Default	
	The count number is 3.
	There is no delay.
	The interval is 30 seconds.
	The ARP probe default source IP address is the Layer 3 interface and 0.0.0.0 for switchports.

Command Modes	
	Global configuration

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

Usage Guidelines	
	Use the use-svi keyword to configure the IP device tracking table to use the SVI IP address for ARP probes in cases when the default source IP address 0.0.0.0 for switch ports is used and the ARP probes drop.

Examples	
	This example shows how to set SVI as the source for ARP probes:

```
Device(config)# ip device tracking probe use-svi
```

ip dhcp snooping database

To configure the Dynamic Host Configuration Protocol (DHCP)-snooping database, use the **ip dhcp snooping database** command in global configuration mode. To disable the DHCP-snooping database, use the **no** form of this command.

```
ip dhcp snooping database {crashinfo:url | flash:url | ftp:url | http:url | https:url | rcp:url
| scp:url | tftp:url | timeout seconds | usbflash0:url | write-delay seconds}
no ip dhcp snooping database [ timeout | write-delay ]
```

Syntax Description

crashinfo:url	Specifies the database URL for storing entries using crashinfo.
flash:url	Specifies the database URL for storing entries using flash.
ftp:url	Specifies the database URL for storing entries using FTP.
http:url	Specifies the database URL for storing entries using HTTP.
https:url	Specifies the database URL for storing entries using secure HTTP (https).
rcp:url	Specifies the database URL for storing entries using remote copy (rcp).
scp:url	Specifies the database URL for storing entries using Secure Copy (SCP).
tftp:url	Specifies the database URL for storing entries using TFTP.
timeout seconds	Specifies the abort timeout interval; valid values are from 0 to 86400 seconds.
usbflash0:url	Specifies the database URL for storing entries using USB flash.
write-delay seconds	Specifies the amount of time before writing the DHCP-snooping entries to an external server after a change is seen in the local DHCP-snooping database; valid values are from 15 to 86400 seconds.

Command Default The DHCP-snooping database is not configured.

Command Modes Global configuration

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

Usage Guidelines You must enable DHCP snooping on the interface before entering this command. Use the **ip dhcp snooping** command to enable DHCP snooping.

This example shows how to specify the database URL using TFTP:

```
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
```


This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
Device(config)# ip dhcp snooping database write-delay 15
```

ip dhcp snooping information option format remote-id

To configure the option-82 remote-ID suboption, use the **ip dhcp snooping information option format remote-id** command in global configuration mode on the switch to configure the option-82 remote-ID suboption. To configure the default remote-ID suboption, use the **no** form of this command.

```
ip dhcp snooping information option format remote-id {hostname | string string}
no ip dhcp snooping information option format remote-id {hostname | string string}
```

Syntax Description	hostname Specify the switch hostname as the remote ID.	
	string string Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).	
Command Default	The switch MAC address is the remote ID.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.
Usage Guidelines	You must globally enable DHCP snooping by using the ip dhcp snooping global configuration command for any DHCP snooping configuration to take effect.	
	When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.	
		
Note	If the hostname exceeds 63 characters, it will be truncated to 63 characters in the remote-ID configuration.	

This example shows how to configure the option- 82 remote-ID suboption:

```
Device(config)# ip dhcp snooping information option format remote-id hostname
```


ip dhcp snooping verify no-relay-agent-address

To disable the DHCP snooping feature from verifying that the relay agent address (giaddr) in a DHCP client message matches the client hardware address on an untrusted port, use the **ip dhcp snooping verify no-relay-agent-address** command in global configuration mode. To enable verification, use the **no** form of this command.

ip dhcp snooping verify no-relay-agent-address
no ip dhcp snooping verify no-relay-agent-address

Syntax Description

This command has no arguments or keywords.

Command Default

The DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0.

Command Modes

Global configuration

Command History

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

Usage Guidelines

By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the **ip dhcp snooping verify no-relay-agent-address** command to disable the verification. Use the **no ip dhcp snooping verify no-relay-agent-address** to reenale verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device(config)# no ip dhcp snooping verify no-relay-agent-address
```

ip http access-class

To specify the access list that should be used to restrict access to the HTTP server, use the **ip http access-class** command in global configuration mode. To remove a previously configured access list association, use the **no** form of this command.



Note The existing **ip http access-class** *access-list-number* command is currently supported, but is going to be deprecated. Use the **ip http access-class ipv4** { *access-list-number* | *access-list-name* } and **ip http access-class ipv6** *access-list-name* instead.

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } |
ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name }
| ipv6 access-list-name }
```

Syntax Description

ipv4	Specifies the IPv4 access list to restrict access to the secure HTTP server.
ipv6	Specifies the IPv6 access list to restrict access to the secure HTTP server.
<i>access-list-number</i>	Standard IP access list number in the range 0 to 99, as configured by the access-list global configuration command.
<i>access-list-name</i>	Name of a standard IPv4 access list, as configured by the ip access-list command.

Command Default

No access list is applied to the HTTP server.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified. The ipv4 and ipv6 keyword were added.
Cisco IOS XE Release 3.3SE	This command was introduced.

Usage Guidelines

If this command is configured, the specified access list is assigned to the HTTP server. Before the HTTP server accepts a connection, it checks the access list. If the check fails, the HTTP server does not accept the request for a connection.

Examples

The following example shows how to define an access list as 20 and assign it to the HTTP server:

```
Device(config)# ip access-list standard 20
Device(config-std-nacl)# permit 209.165.202.130 0.0.0.255
Device(config-std-nacl)# permit 209.165.201.1 0.0.255.255
```

```
Device(config-std-nacl)# permit 209.165.200.225 0.255.255.255
Device(config-std-nacl)# exit
Device(config)# ip http access-class 20
```

The following example shows how to define an IPv4 named access list as and assign it to the HTTP server.

```
Device(config)# ip access-list standard Internet_filter
Device(config-std-nacl)# permit 1.2.3.4
Device(config-std-nacl)# exit
Device(config)# ip http access-class ipv4 Internet_filter
```

Related Commands

Command	Description
ip access-list	Assigns an ID to an access list and enters access list configuration mode.
ip http server	Enables the HTTP 1.1 server, including the Cisco web browser user interface.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface *interface-name* [**vrf** *vrf-name*]
no ip radius source-interface

Syntax Description	
<i>interface-name</i>	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf <i>vrf-name</i>	(Optional) Per virtual route forwarding (VRF) configuration.

Command Default No default behavior or values.

Command Modes Global configuration (config)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines Use this command to set the IP address of an interface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the interface is in the *up* state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. RADIUS uses the IP address of the interface that it is associated to, regardless of whether the interface is in the *up* or *down* state.

The **ip radius source-interface** command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified interface should have a valid IP address and should be in the *up* state for a valid configuration. If the specified interface does not have a valid IP address or is in the *down* state, RADIUS selects a local IP that corresponds to the best possible route to the AAA server. To avoid this, add a valid IP address to the interface or bring the interface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple disjointed routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

Examples

The following example shows how to configure RADIUS to use the IP address of interface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of interface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet0 vrf vrf1
```

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:

```
Device# configure terminal
Deviceconfig) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
```

ip verify source

To enable IP source guard on an interface, use the **ip verify source** command in interface configuration mode. To disable IP source guard, use the **no** form of this command.

```
ip verify source [mac-check][tracking]
no ip verify source
```

Syntax Description

mac-check (Optional) Enables IP source guard with MAC address verification.

tracking (Optional) Enables IP port security to learn static IP address learning on a port.

Command Default

IP source guard is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

To enable IP source guard with source IP address filtering, use the **ip verify source** interface configuration command.

To enable IP source guard with source IP address filtering and MAC address verification, use the **ip verify source mac-check** interface configuration command.

Examples

This example shows how to enable IP source guard with source IP address filtering on an interface:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
```

This example shows how to enable IP source guard with MAC address verification:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
```

You can verify your settings by entering the **show ip verify source** privileged EXEC command.

ipv6 access-list

To define an IPv6 access list and to place the device in IPv6 access list configuration mode, use the **ipv6 access-list** command in global configuration mode. To remove the access list, use the **no** form of this command.

ipv6 access-list *access-list-name* | **match-local-traffic** | **log-update threshold** *threshold-in-msgs* | **role-based** *list-name*
noipv6 access-list *access-list-name* | **client permit-control-packets** | **log-update** *threshold* | **role-based** *list-name*

Syntax Description

ipv6 <i>access-list-name</i>	Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode. <i>access-list-name</i> - Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.
match-local-traffic	Enables matching for locally-generated traffic.
log-update threshold <i>threshold-in-msgs</i>	Determines how syslog messages are generated after the initial packet match. <i>threshold-in-msgs</i> - Number of packets generated.
role-based <i>list-name</i>	Creates a role-based IPv6 ACL.

Command Default

No IPv6 access list is defined.

Command Modes

Global configuration

Command History

Release	Modification
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

IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Configuring the **ipv6 access-list** command places the device in IPv6 access list configuration mode--the device prompt changes to Device(config-ipv6-acl)#. From IPv6 access list configuration mode, permit and deny conditions can be set for the defined IPv6 ACL.



Note

IPv6 ACLs are defined by a unique name (IPv6 does not support numbered ACLs). An IPv4 ACL and an IPv6 ACL cannot share the same name.

IPv6 is automatically configured as the protocol type in **permit any any** and **deny any any** statements that are translated from global configuration mode to IPv6 access list configuration mode.

Every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Use the **ipv6 traffic-filter** interface configuration command with the *access-list-name* argument to apply an IPv6 ACL to an IPv6 interface. Use the **ipv6 access-class** line configuration command with the *access-list-name* argument to apply an IPv6 ACL to incoming and outgoing IPv6 virtual terminal connections to and from the device.

An IPv6 ACL applied to an interface with the **ipv6 traffic-filter** command filters traffic that is forwarded, not originated, by the device.

Examples

The example configures the IPv6 ACL list named list1 and places the device in IPv6 access list configuration mode.

```
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)#
```

The following example configures the IPv6 ACL named list2 and applies the ACL to outbound traffic on Ethernet interface 0. Specifically, the first ACL entry keeps all packets from the network FEC0:0:0:2::/64 (packets that have the site-local prefix FEC0:0:0:2 as the first 64 bits of their source IPv6 address) from exiting out of Ethernet interface 0. The second entry in the ACL permits all other traffic to exit out of Ethernet interface 0. The second entry is necessary because an implicit deny all condition is at the end of each IPv6 ACL.

```
Device(config)# ipv6 access-list list2 deny FEC0:0:0:2::/64 any
Device(config)# ipv6 access-list list2 permit any any
Device(config)# interface ethernet 0
Device(config-if)# ipv6 traffic-filter list2 out
```

ipv6 snooping policy



Note All existing IPv6 Snooping commands (prior to Cisco IOS XE Denali 16.1.1) now have corresponding SISF-based device-tracking commands that allow you to apply your configuration to both IPv4 and IPv6 address families. For more information, 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:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)#
```

key chain macsec

To configure a MACsec key chain name on a device interface to fetch a Pre Shared Key (PSK), use the **key chain macsec** command in global configuration mode. To disable it, use the **no** form of this command.

key chain *name* **macsec** {**description** | **key** | **exit**}

Syntax Description	
name	Name of a key chain to be used to get keys.
description	Provides description of the MACsec key chain.
key	Configure a MACsec key.
exit	Exits from the MACsec key-chain configuration mode.
no	Negates the command or sets the default values.

Command Default key chain macsec is disabled.

Command Modes Global configuration

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

This example shows how to configure MACsec key chain to fetch a 128-bit Pre Shared Key (PSK):

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 1000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-128-cmac
Switch(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Switch(config-keychain-macsec-key)#end
Switch#
```

This example shows how to configure MACsec key chain to fetch a 256-bit Pre Shared Key (PSK):

```
Switch#configure terminal
Switch(config)#key chain kcl macsec
Switch(config-keychain-macsec)#key 2000
Switch(config-keychain-macsec)#cryptographic-algorithm aes-256-cmac
Switch(config-keychain-macsec-key)# key-string
c865632acb269022447c417504a1bf5db1c296449b52627ba01f2ba2574c2878
Switch(config-keychain-macsec-key)#end
Switch#
```

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:

```
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
```

mab request format attribute 32

To enable VLAN ID-based MAC authentication on a switch, use the **mab request format attribute 32 vlan access-vlan** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
mab request format attribute 32 vlan access-vlan
no mab request format attribute 32 vlan access-vlan
```

Syntax Description	This command has no arguments or keywords.	
Command Default	VLAN-ID based MAC authentication is disabled.	
Command Modes	Global configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines Use this command to allow a RADIUS server to authenticate a new user based on the host MAC address and VLAN.

Use this feature on networks with the Microsoft IAS RADIUS server. The Cisco ACS ignores this command.

This example shows how to enable VLAN-ID based MAC authentication on a switch:

```
Device(config)# mab request format attribute 32 vlan access-vlan
```

Related Commands	Command	Description
	authentication event	Sets the action for specific authentication events.
	authentication fallback	Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.
	authentication host-mode	Sets the authorization manager mode on a port.
	authentication open	Enables or disables open access on a port.
	authentication order	Sets the order of authentication methods used on a port.
	authentication periodic	Enables or disables reauthentication on a port.
	authentication port-control	Enables manual control of the port authorization state.
	authentication priority	Adds an authentication method to the port-priority list.

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.

macsec network-link

To enable MKA MACsec configuration on the uplink interfaces, use the **macsec network-link** command on the interface. To disable it, use the **no** form of this command.

macsec network-link

Syntax Description	macsec network-link Enables MKA MACsec configuration on device interfaces using EAP-TLS authentication protocol.				
Command Default	macsec network-link is disabled.				
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 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.				

This example shows how to configure MACsec MKA on an interface using the EAP-TLS authentication protocol:

```
Switch#configure terminal
Switch(config)# int G1/0/20
Switch(config-if)# macsec network-link
Switch(config-if)# end
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:

```
Device(config)# vlan access-map vmap4
Device(config-access-map)# match ip address al2
Device(config-access-map)# action drop
```



```
Device(config-access-map)# exit  
Device(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

mka policy (global configuration)

To create a MACsec Key Agreement (MKA) protocol policy and to enter MKA policy configuration mode, use the **no** form of this command. **mka policy** command in global configuration mode. To delete the policy, use the **no** form of this command.

mka policy *policy-name*
no mka policy *policy-name*

Syntax Description	<i>policy-name</i> Identifies an MKA policy and enters MKA policy configuration mode. The maximum length for the policy name is 16 characters.
---------------------------	--

Command Default No MKA policies are created.

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 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.				

Usage Guidelines If you enter the name of an existing policy, you see a warning that any changes to the policy deletes all active MKA sessions with that policy. Whenever you change an MKA policy, active MKA sessions with that policy applied are cleared. If you try to create a policy name with more than 16 characters, you see a warning message, and the policy is not created.

If you enter the **no mka policy** *policy-name* command to delete a policy that is applied to at least one interface, you are prompted to first remove the policy from all interfaces that it is applied to and then to reenter the command. If you attempt to delete a policy and the policy name does not exist, you are notified.

When you enter MKA policy mode, these commands are available:

- confidentiality-offset—Sets the confidentiality offset for MACsec operation
- replay-protection—Configures MKA to use replay protection for MACsec operation

Examples

The following example shows how to configure an MKA policy and what you see if you create a policy name that already exists:

```
Device(config)# mka policy test-policy
Device(config-mka-policy)# exit
Device(config)# mka policy test-policy
%MKA policy "test-policy" may have associated active MKA Sessions.
Changes to MKA Policy "test-policy" values
will cause all associated active MKS Sessions to be cleared.
```

Related Commands

Command	Description
mka policy (interface configuration)	Applies an MKA policy to an interface.
show mka policy	Displays information about defined MKA protocol policies.

mka pre-shared-key

To configure MKA MACsec on a device interface using a Pre Shared Key (PSK), use the **mka pre-shared-key key-chain** *key-chain name* command in global configuration mode. To disable it, use the **no** form of this command.

mka pre-shared-key key-chain *key-chain-name*

Syntax Description	mka pre-shared-key key-chain Enables MACsec MKA configuration on device interfaces using a PSK.	
Command Default	mka pre-shared-key is disabled.	
Command Modes	Interface configuration	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

This example shows how to configure MKA MACsec on an interface using a PSK:

```
Switch#
Switch(config)# int G1/0/20
Switch(config-if)# mka pre-shared-key key-chain kcl
Switch(config-if)# end
Switch#
```

no authentication logging verbose

To filter detailed information from authentication system messages, use the **no authentication logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no authentication logging verbose

Syntax Description This command has no arguments or keywords.

Command Default All details are not displayed in the system messages.

Command Modes Global configuration

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

Usage Guidelines This command filters details, such as anticipated success, from authentication system messages. Failure messages are not filtered.

To filter verbose authentication system messages:

```
Device(config)# no authentication logging verbose
```

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

Related Commands	Command	Description
	no authentication logging verbose	Filters details from authentication system messages.
	no dot1x logging verbose	Filters details from 802.1x system messages.
	no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **no dot1x logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no dot1x logging verbose

Syntax Description This command has no arguments or keywords.

Command Default All details are not displayed in the system messages.

Command Modes Global configuration

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

Usage Guidelines This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

To filter verbose 802.1x system messages:

```
Device(config)# no dot1x logging verbose
```

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

Related Commands	Command	Description
	no authentication logging verbose	Filters details from authentication system messages.
	no dot1x logging verbose	Filters details from 802.1x system messages.
	no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

no mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the **no mab logging verbose** command in global configuration mode on the switch stack or on a standalone switch.

no mab logging verbose

Syntax Description This command has no arguments or keywords.

Command Default All details are not displayed in the system messages.

Command Modes Global configuration

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

Usage Guidelines This command filters details, such as anticipated success, from MAC authentication bypass (MAB) system messages. Failure messages are not filtered.

To filter verbose MAB system messages:

```
Device(config)# no mab logging verbose
```

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

Related Commands	Command	Description
	no authentication logging verbose	Filters details from authentication system messages.
	no dot1x logging verbose	Filters details from 802.1x system messages.
	no mab logging verbose	Filters details from MAC authentication bypass (MAB) system messages.

permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the **permit** MAC access-list configuration command on the switch stack or on a standalone switch. To remove a permit condition from the extended MAC access list, use the **no** form of this command.

```
{permit {any | 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 | lavc-sca | lsaplsap 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 | lavc-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.
lavc-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 39: IPX Filtering Criteria

IPX Encapsulation Type		Filter Criterion
Cisco IOS Name	Novell Name	
arpa	Ethernet II	EtherType 0x8137
snap	Ethernet-snap	EtherType 0x8137
sap	Ethernet 802.2	LSAP 0xE0E0
novell-ether	Ethernet 802.3	LSAP 0xFFFF

This example shows how to define the MAC-named extended access list to allow NetBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with EtherType 0x4321:

```
Device(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

Related Commands

Command	Description
deny	Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.
mac access-list extended	Creates an access list based on MAC addresses for non-IP traffic.

Command	Description
show access-lists	Displays access control lists configured on a switch.

propagate sgt (cts manual)

To enable Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces, use the **propagate sgt** command in interface configuration mode. To disable SGT propagation, use the **no** form of this command.

propagate sgt

Syntax Description	This command has no arguments or keywords.
Command Default	SGT processing propagation is enabled.
Command Modes	CTS manual interface configuration mode (config-if-cts-manual)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines SGT processing propagation allows a CTS-capable interface to accept and transmit a CTS Meta Data (CMD) based L2 SGT tag. The **no propagate sgt** command can be used to disable SGT propagation on an interface in situations where a peer device is not capable of receiving an SGT, and as a result, the SGT tag cannot be put in the L2 header.

Examples

The following example shows how to disable SGT propagation on a manually-configured TrustSec-capable interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Switch#show cts interface brief
Global Dot1x feature is Disabled
Interface GigabitEthernet0:
  CTS is enabled, mode:      MANUAL
  IFC state:                 OPEN
  Authentication Status:    NOT APPLICABLE
  Peer identity:             "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:     NOT APPLICABLE
  SAP Status:                NOT APPLICABLE
  Propagate SGT:            Disabled
  Cache Info:
    Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.

Command	Description
show cts interface	Displays Cisco TrustSec states and statistics per interface.

protocol (IPv6 snooping)

To specify that addresses should be gleaned with Dynamic Host Configuration Protocol (DHCP) or Neighbor Discovery Protocol (NDP), or to associate the protocol with an IPv6 prefix list, use the **protocol** command. To disable address gleaning with DHCP or NDP, use the **no** form of the command.

```
protocol { dhcp | ndp }
no protocol { dhcp | ndp }
```

Syntax Description

dhcp Specifies that addresses should be gleaned in Dynamic Host Configuration Protocol (DHCP) packets.

ndp Specifies that addresses should be gleaned in Neighbor Discovery Protocol (NDP) packets.

Command Default

Snooping and recovery are attempted using both DHCP and NDP.

Command Modes

IPv6 snooping configuration mode

Command History

Release

Cisco IOS XE 3.2SE

Modification

This command was introduced.

Usage Guidelines

If an address does not match the prefix list associated with DHCP or NDP, then control packets will be dropped and recovery of the binding table entry will not be attempted with that protocol.

- Using the **no protocol** { **dhcp** | **ndp** } command indicates that a protocol will not be used for snooping or gleaning.
- If the **no protocol dhcp** command is used, DHCP can still be used for binding table recovery.
- Data glean can recover with DHCP and NDP, though destination guard will only recovery through DHCP.

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to use DHCP to glean addresses:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
```

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 { <i>ipv4</i> <i>ipv6</i> }	<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:

```
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
```


sap mode-list (cts manual)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

Use the **sap mode-list** command to manually specify the Pairwise Master Key (PMK) and the Security Association Protocol (SAP) authentication and encryption modes to negotiate MACsec link encryption between two interfaces. Use the **no** form of the command to disable the configuration.

sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

no sap pmk mode-list {gcm-encrypt | gmac | no-encap | null} [gcm-encrypt | gmac | no-encap | null]

Syntax Description		
	pmk <i>hex_value</i>	Specifies the Hex-data PMK (without leading 0x; enter even number of hex characters, or else the last character is prefixed with 0.).
	mode-list	Specifies the list of advertised modes (prioritized from highest to lowest).
	gcm-encrypt	Specifies GMAC authentication, GCM encryption.
	gmac	Specifies GMAC authentication only, no encryption.
	no-encap	Specifies no encapsulation.
	null	Specifies encapsulation present, no authentication, no encryption.

Command Default The default encryption is **sap pmk mode-list gcm-encrypt null**. When the peer interface does not support 802.1AE MACsec or 802.REV layer-2 link encryption, the default encryption is **null**.

Command Modes CTS manual interface configuration (config-if-cts-manual)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use the **sap pmk mode-list** command to specify the authentication and encryption method.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

SAP and the Pairwise Master Key (PMK) can be manually configured between two interfaces with the **sap pmk mode-list** command. When using 802.1X authentication, both sides (supplicant and authenticator) receive the PMK and the MAC address of the peer's port from the Cisco Secure Access Control Server.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

Examples

The following example shows how to configure SAP on a Gigabit Ethernet interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk FFEED mode-list gcm-encrypt
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
show cts interface	Displays Cisco TrustSec interface configuration statistics.

security level (IPv6 snooping)

To specify the level of security enforced, use the **security-level** command in IPv6 snooping policy configuration mode.

security level { **glean** | **guard** | **inspect** }

Syntax Description	glean	Extracts addresses from the messages and installs them into the binding table without performing any verification.
	guard	Performs both glean and inspect. Additionally, RA and DHCP server messages are rejected unless they are received on a trusted port or another policy authorizes them.
	inspect	Validates messages for consistency and conformance; in particular, address ownership is enforced. Invalid messages are dropped.
Command Default	The default security level is guard.	
Command Modes	IPv6 snooping configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to define an IPv6 snooping policy name as policy1, place the device in IPv6 snooping configuration mode, and configure the security level as inspect:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
```

security passthru

To modify the IPsec pass-through, use the **security passthru** command. To disable, use the no form of the command.

```
security passthru ip-address
no security passthru
```

Syntax Description	<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	<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 modify IPsec pass-through.

```
Device#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)#security passthrough 10.1.1.1
```

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

no server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

<i>ip-address</i>	IP address of the private RADIUS server host.
auth-port <i>port-number</i>	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port <i>port-number</i>	(Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout <i>seconds</i>	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used.
retransmit <i>retries</i>	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
key <i>string</i>	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. The <i>string</i> can be 0 (specifies that an unencrypted key follows), 6 (specifies that an advanced encryption scheme [AES] encrypted key follows), 7 (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

RADIUS server-group configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwarding (VRF) instances, private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

**Note**

- If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private (RADIUS)** command.
- Creating or updating AAA server statistics record for private RADIUS servers are not supported. If private RADIUS servers are used, then error messages and tracebacks will be encountered, but these error messages or tracebacks do not have any impact on the AAA RADIUS functionality. To avoid these error messages and tracebacks, configure public RADIUS server instead of private RADIUS server.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
password encryption aes	Enables a type 6 encrypted preshared key.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users to log in to a Cisco NAS and select a RADIUS server for authentication.

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

Cisco IOS XE 3.2SE

Modification

This command was introduced.

This is an example of output from the **show aaa clients** command:

```
Device# show aaa clients
Dropped request packets: 0
```

show aaa command handler

To show AAA command handler statistics, use the **show aaa command handler** command.

show aaa command handler

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC

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

This is an example of output from the **show aaa command handler** command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
account-logon: 0, account-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:

```
Device# show aaa local statistics

Local EAP statistics

EAP Method          Success      Fail
-----
Unknown              0            0
EAP-MD5              0            0
EAP-GTC              0            0
LEAP                 0            0
PEAP                 0            0
EAP-TLS              0            0
EAP-MSCHAPV2        0            0
EAP-FAST             0            0

Requests received from AAA:          0
Responses returned from EAP:        0
Requests dropped (no EAP AVP):      0
Requests dropped (other reasons):    0
Authentication timeouts from EAP:   0

Credential request statistics
Requests sent to backend:            0
Requests failed (unable to send):    0
Authorization results received

Success:                              0
Fail:                                  0
```

show aaa servers

To show all AAA servers as seen by the AAA server MIB, use the **show aaa servers** command.

show aaa servers [**private** | **public** | [**detailed**]]

Syntax Description		
	detailed	(Optional) Displays private AAA servers as seen by the AAA Server MIB.
	public	(Optional) Displays public AAA servers as seen by the AAA Server MIB.
	detailed	(Optional) Displays detailed AAA server statistics.
Command Modes	User EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

This is an example of output from the **show aaa servers** command:

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 172.20.128.2, auth-port 1645, acct-port 1646
State: current UP, duration 9s, previous duration 0s
Dead: total time 0s, count 0
Quarantined: No
Authen: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
Response: accept 0, reject 0, challenge 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Account: request 0, timeouts 0, failover 0, retransmission 0
Request: start 0, interim 0, stop 0
Response: start 0, interim 0, stop 0
Response: unexpected 0, server error 0, incorrect 0, time 0ms
Transaction: success 0, failure 0
Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 0m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
```

show aaa sessions

To show AAA sessions as seen by the AAA Session MIB, use the **show aaa sessions** command.

show aaa sessions

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	User EXEC
----------------------	-----------

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

This is an example of output from the **show aaa sessions** command:

```
Device# show aaa sessions
Total sessions since last reload: 7
Session Id: 4007
  Unique Id: 4025
  User Name: *not available*
  IP Address: 0.0.0.0
  Idle Time: 0
  CT Call Handle: 0
```

show authentication history

To display the authenticated sessions alive on the device, use the **show authentication history** command.

show authentication history [**min-uptime** *seconds*]

Syntax Description

min-uptime *seconds* (Optional) Displays sessions within the minimum uptime. The range is from 1 through 4294967295 seconds.

Command Modes

User EXEC

Command History

Release

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:

```
Device# show authentication history
Interface  MAC Address      Method  Domain  Status  Uptime
Gi3/0/2    0021.d864.07c0  dot1x   DATA   Auth    38s

Session count = 1
```

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

```
show authentication sessions [database] [handle handle-id [details]] [interface type number
[details] [mac mac-address [interface type number] [method method-name [interface type number
[details] [session-id session-id [details]]]
```

Syntax Description

database	(Optional) Shows only data stored in session database.
handle <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 40: 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 41: Authentication Method States

State	Description
dot1x	802.1X
mab	MAC authentication bypass
webauth	web authentication

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions
Interface  MAC Address  Method  Domain  Status  Session ID
Gi1/0/48   0015.63b0.f676  dot1x   DATA   Authz Success  0A3462B1000000102983C05C
Gi1/0/5    000f.23c4.a401  mab     DATA   Authz Success  0A3462B10000000D24F80B58
Gi1/0/5    0014.bf5d.d26d  dot1x   DATA   Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface gigabitethernet2/0/47
      Interface: GigabitEthernet2/0/47
      MAC Address: Unknown
      IP Address: Unknown
      Status: Authz Success
      Domain: DATA
      Oper host mode: multi-host
      Oper control dir: both
      Authorized By: Guest Vlan
      Vlan Policy: 20
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 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 cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface, use the **show cts interface** command in EXEC or privileged EXEC mode.

show cts interface [{**type** *slot/port* | **brief** | **summary**}]

Syntax Description

type <i>slot/port</i>	(Optional) Specifies an interface type and slot or port number. A verbose output for this interface is returned.
brief	(Optional) Displays abbreviated status for all CTS interfaces.
summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

Command Default

None

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was modified with additional options.
Cisco IOS XE Denali 16.2.1	This command was introduced.

Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples

The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Switch# show cts interface

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:18.232
  Authentication Status:  NOT APPLICABLE
    Peer identity:        "unknown"
    Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Configured pairwise ciphers:
    gcm-encrypt
    null

  Replay protection:      enabled
  Replay protection mode: STRICT

  Selected cipher:
```



```

Propagate SGT:          Enabled
Cache Info:
  Cache applied to link : NONE

Statistics:
  authc success:        0
  authc reject:         0
  authc failure:        0
  authc no response:    0
  authc logoff:         0
  sap success:          0
  sap fail:             0
  authz success:        0
  authz fail:           0
  port auth fail:      0
Ingress:
  control frame bypassed: 0
  sap frame bypassed:    0
  esp packets:           0
  unknown sa:           0
  invalid sa:            0
  inverse binding failed: 0
  auth failed:           0
  replay error:         0
Egress:
  control frame bypassed: 0
  esp packets:           0
  sgt filtered:          0
  sap frame bypassed:    0
  unknown sa dropped:    0
  unknown sa bypassed:   0

```

The following example displays output using the **brief** keyword:

```

Device# show cts interface brief

Global Dot1x feature is Disabled
Interface GigabitEthernet0/1/0:
  CTS is enabled, mode:    MANUAL
  IFC state:              OPEN
  Interface Active for 00:00:40.386
  Authentication Status:  NOT APPLICABLE
  Peer identity:          "unknown"
  Peer's advertised capabilities: ""
  Authorization Status:   NOT APPLICABLE
  SAP Status:             NOT APPLICABLE
  Propagate SGT:          Enabled
  Cache Info:
    Cache applied to link : NONE

```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
propagate sgt (cts manual)	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.
sap mode-list (cts manual)	Manually specifies the PMK and the SAP authentication and encryption modes to negotiate MACsec link encryption between two interfaces.

show cts role-based permissions

To display the role-based (security group) access control permission list, use the **show cts role-based permissions** command in privileged EXEC mode.

```
show cts role-based permissions [{default [{details | ipv4 [{details}]}] | from [{sgt [{ipv4 | to [{sgt | unknown}]}] [{details | ipv4 [{details}]}]}] | unknown}] | ipv4 | to [{sgt | unknown}] [{ipv4}]
```

Syntax Description

default	(Optional) Displays information about the default permission list.
details	(Optional) Displays attached access control list (ACL) details.
ipv4	(Optional) Displays information about the IPv4 protocol.
from	(Optional) Displays information about the source group.
<i>sgt</i>	(Optional) Security Group Tag. Valid values are from 2 to 65519.
to	(Optional) Displays information about the destination group.
unknown	(Optional) Displays information about unknown source and destination groups.

Command Modes

Privileged EXE (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines

This command displays the content of the SGACL permission matrix. You can specify the source security group tag (SGT) by using the **from** keyword and the destination SGT by using the **to** keyword. When both these keywords are specified RBACLs of a single cell are displayed. An entire column is displayed when only the **to** keyword is used. An entire row is displayed when the **from** keyword is used. The entire permission matrix is displayed when both the **from** and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. SGACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco Identity Services Engine (ISE).

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the access control entries of SGACLs of a single cell are displayed.

The following is sample output from the **show role-based permissions** command:

```
Switch# show cts role-based permissions

IPv4 Role-based permissions default (monitored):
default_sgacl-02
Permit IP-00
IPv4 Role-based permissions from group 305:sgt to group 306:dgt (monitored):
test_reg_tcp_permit-02
RBACL Monitor All for Dynamic Policies : TRUE
RBACL Monitor All for Configured Policies : FALSE
```

```
IPv4 Role-based permissions from group 6:SGT_6 to group 6:SGT_6 (configured):  
  mon_1  
IPv4 Role-based permissions from group 10 to group 11 (configured):  
  mon_2  
RBACL Monitor All for Dynamic Policies : FALSE  
RBACL Monitor All for Configured Policies : FALSE
```

Related Commands

Command	Description
cts role-based permissions	Enables permissions from a source group to a destination group.
cts role-based monitor	Enables role-based access list monitoring.

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:

```
Device# show cisp interface fast 0
CISP not enabled on specified interface
```

This example shows output from the **show cisp registration** command:

```
Device# 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:

```
Device# show dot1x all
Sysauthcontrol           Enabled
Dot1x Protocol Version   3
```

This is an example of output from the **show dot1x all count** command:

```
Device# show dot1x all count
Number of Dot1x sessions
-----
Authorized Clients       = 0
UnAuthorized Clients     = 0
Total No of Client       = 0
```

This is an example of output from the **show dot1x all statistics** command:

```
Device# show dot1x statistics
Dot1x Global Statistics for
-----
RxStart = 0      RxLogoff = 0      RxResp = 0      RxRespID = 0
RxReq = 0        RxInvalid = 0    RxLenErr = 0
RxTotal = 0
```

```
TxStart = 0      TxLogoff = 0      TxResp = 0
TxReq = 0        ReTxReq = 0        ReTxReqFail = 0
TxReqID = 0      ReTxReqID = 0      ReTxReqIDFail = 0
TxTotal = 0
```

show eap pac peer

To display stored Protected Access Credentials (PAC) for Extensible Authentication Protocol (EAP) Flexible Authentication via Secure Tunneling (FAST) peers, use the **show eap pac peer** command in privileged EXEC mode.

show eap pac peer

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

This is an example of output from the **show eap pac peers** privileged EXEC command:

```
Device> show eap pac peers
No PACs stored
```

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show ip dhcp snooping statistics

To display DHCP snooping statistics in summary or detail form, use the **show ip dhcp snooping statistics** command in user EXEC mode.

show ip dhcp snooping statistics [**detail**]

Syntax Description

detail (Optional) Displays detailed statistics information.

Command Modes

User EXEC

Command History

Release

Cisco IOS XE 3.2SE

Modification

This command was introduced.

Usage Guidelines

In a switch stack, all statistics are generated on the stack master. If a new active switch is elected, the statistics counters reset.

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Device> show ip dhcp snooping statistics

Packets Forwarded                = 0
Packets Dropped                  = 0
Packets Dropped From untrusted ports = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Device> show ip dhcp snooping statistics detail

Packets Processed by DHCP Snooping = 0
Packets Dropped Because
  IDB not known                    = 0
  Queue full                        = 0
  Interface is in errdisabled       = 0
  Rate limit exceeded               = 0
  Received on untrusted ports       = 0
  Nonzero giaddr                    = 0
  Source mac not equal to chaddr     = 0
  Binding mismatch                  = 0
  Insertion of opt82 fail           = 0
  Interface Down                    = 0
  Unknown output interface          = 0
  Reply output port equal to input port = 0
  Packet denied by platform         = 0
```

This table shows the DHCP snooping statistics and their descriptions:

Table 42: 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 macsec

To display 802.1ae Media Access Control Security (MACsec) information, use the **show macsec** command in privileged EXEC mode.

show macsec {*interface**interface-id* | **summary**}

Syntax Description	interface <i>interface-id</i>	Displays MACsec interface details.
	summary	Displays MACsec summary information.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

This is sample output of the **show macsec interface** command when there is no MACsec session established on the interface:

```
Switch# show macsec interface gigabitethernet 1/0/1
MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
  No Transmit Secure Channels
  No Receive Secure Channels
```

This is sample output of the **show macsec interface** command after the session is established:

```
Switch# show macsec interface gigabitethernet 1/0/1
MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
```

```

Transmit Secure Channels
SCI : 0022BDCF9A010002
Elapsed time : 00:00:00
Current AN: 0 Previous AN: -1
SC Statistics
Auth-only (0 / 0)
Encrypt (1910 / 0)
Receive Secure Channels
SCI : 001B2140EC4C0000
Elapsed time : 00:00:00
Current AN: 0 Previous AN: -1
SC Statistics
Notvalid pkts 0 Invalid pkts 0
Valid pkts 1 Late pkts 0
Uncheck pkts 0 Delay pkts 0
Port Statistics
Ingress untag pkts 0 Ingress notag pkts 1583
Ingress badtag pkts 0 Ingress unknownSCI pkts 0
Ingress noSCI pkts 0 Unused pkts 0
Notusing pkts 0 Decrypt bytes 80914
Ingress miss pkts 1492

```

This is sample output of the **show macsec summary** command to see all established MACsec sessions:

```

Switch# show macsec summary
Interface          Transmit SC      Receive SC
GigabitEthernet1/0/18      0                0
GigabitEthernet1/0/20      1                1
GigabitEthernet1/0/21      0                0
GigabitEthernet1/0/22      1                1
GigabitEthernet4/0/19      0                0
GigabitEthernet4/0/20      1                1
GigabitEthernet4/0/22      0                0

```

Related Commands

Command	Description
macsec	Enables MACsec on an interface

show mka policy

To display a summary of all defined MACsec Key Agreement (MKA) protocol policies, including the MKA default policy, or to display a summary of a specified policy, use the **show mka policy** command in privileged EXEC mode.

show mka policy [*policy-name*] [**detail**] [**sessions**]

Syntax Description		
	<i>policy-name</i>	(Optional) Specifies the name for the policy.
	detail	(Optional) Displays detailed configuration information for the specified MKA policy, including the names of the physical interfaces to which the policy is applied. The output shows the default values for each configuration option. When entered after the session keyword, displays detailed status information about all active MKA sessions with the specified policy name.
	sessions	(Optional) Displays a summary of all active MKA sessions with the specified policy name.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

This is sample output of the **show mka policy** command:

```
Switch# show mka policy
MKA Policy Summary...
Policy      KS      Delay  Replay  Window  Conf  Interfaces
Name       Priority Protect Protect Size    Offset Applied
=====
*DEFAULT POLICY* 0      NO     YES     0      0     Gi1/0/1
MkaPolicy-1  0      NO     YES     1000   0     Gi1/0/2  Gi1/0/3
MkaPolicy-2  0      NO     YES     0      50    Gi1/0/4  Gi1/0/5
MkaPolicy-3  0      YES    YES     64     30    Gi1/0/4  Gi1/0/6
my_policy   0      NO     YES     4294967295 0
test-policy 0      NO     YES     10000  0
```

Table 43: Table 0-5 show mka policy Output Fields

Field	Description
Policy Name	The string identifier of the policy.
KS Priority	The set value of the priority for becoming the key server (KS). The range is 0 to 255, with 0 as the highest priority and 255 as the lowest priority. A value of 0 means that the switch should always try to act as the key server, while a value of 255 means that it should never try to act as the server. This value is not configurable.
Delay Protect	The set value of delay protection being provided. This value is not configurable.
Replay Protect	The configured value of replay protection being provided. (This is configurable by entering the replay-protection window-size command.)
Window Size	The configured size of the replay protection window in number of frames per packet. If replay protection is off, the value is 0. If replay protection is on and the value is 0, a strict in-order verification of MACsec frames occurs. (This is configurable by entering the replay-protection window-size command.)
Conf Offset	The configured value of the confidentiality offset in the number of bytes to offset protection or encryption into each frame in MACsec. Configurable values are 0 (no offset), 30, or 50 bytes.
Interfaces Applied	The short name of each interface on which this policy is applied. The string is empty if it is not applied to any interfaces.

This is sample output of the **show mka policy detail** command:

```
Switch# show mka policy MkaPolicy detail
MKA Policy Configuration ("MkaPolicy-3")
=====
MKA Policy Name..... MkaPolicy-3
Key Server Priority.... 0
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size.... 64
Confidentiality Offset. 30
Applied Interfaces...
  GigabitEthernet1/0/4   GigabitEthernet1/0/5
  GigabitEthernet1/0/6
```

This is sample output of the **show mka policy sessions** command:

```

Switch# show mka policy replay-policy sessions
Summary of All Active MKA Sessions with MKA Policy "replay-policy"...
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI       Key-Svr Status   CKN
=====
Gi1/0/25  001b.2140.ec3c/0000 replay-policy    0A05783B0000001700448BA8
2         001e.bdfe.6d99/0002 YES      Secured        3808F996026DFB8A2FCEC9A88BBD0680

```

Related Commands

Command	Description
mka policy (global configuration)	Creates an MKA policy and enters MKA policy configuration mode.
mka policy (interface configuration)	Applies an MKA policy to the interface.

show mka session

To display a summary of active MACsec Key Agreement (MKA) Protocol sessions, use the **show mka session** command in privileged EXEC mode.

show mka session [**interface** *interface-id*] [**port-id** *port-id*] [**local-sci** *sci*] [**detail**]

Syntax Description		
interface <i>interface-id</i>		(Optional) Displays status information for active MKA sessions on an interface.
port-id <i>port-id</i>		(Optional) Displays a summary of active MKA sessions running on the interface with the specified port ID. To see the port ID, enter the show mka session interface interface-id command. Port identifier values begin at 2 and monotonically increase for each new session that uses a virtual port on the same physical interface.
local-sci <i>sci</i>		(Optional) Displays status information for the MKA session identified by the Local TX-SCI. To determine the Local TX-SCI for a specific session, enter the show mka session command without any keywords. The SCI must be 8 octets (16 hexadecimal digits) long.
detail		(Optional) Displays detailed status information about all active MKA sessions, all sessions on the specified interface, or on the specified interface with the specified port ID.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

This is sample output of the **show mka session** command:

```
Switch# show mka session
Total MKA Sessions..... 1
    Secured Sessions... 1
    Pending Sessions... 0
=====
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status    CKN
=====
Gi1/0/1  001b.213d.28ed/0000 *DEFAULT POLICY* 02020202000000000000EAA6
2        001e.bdfe.8402/0002 YES      Secured  3A06ECB1183E42BB4D7817EB2B949D0E
```

```

Gi1/0/1  001a.323a.38ef/0000 *DEFAULT POLICY* 02020314000000000000EAB9
3        001e.bdfc.8402/0003 YES      Pending  CFB1E3B513344AB3417E17FBCB449D3A
Gi1/0/2  001c.113f.2d3a/0000 MkaPolicy-1 02020533000000000000EC81
2        001e.bdfc.8402/0002 YES      Secured  F103EABB133F4AB3497312EF2A949A03

```

Table 44: Table 0-6 show mka session Output Fields

Field	Description
Interface	The short name of the physical interface on which the MKA session is active.
Peer-RxSCI	The MAC address of the interface of the peer concatenated with the peer 16-bit Port-ID.
Policy-name	The name of the policy used at session start to set initial configuration values.
Audit session ID	Session ID.
Port-ID	The Port-ID used in the Local-TX-SCI.
Local-TxSCI	The MAC address of the physical interface concatenated with the 16-bit Port-ID.
Key Server Status	The key server: has value 'Y' for YES if the MKA session is the key server, otherwise, 'N' for NO.
CKN	Connectivity association key (CAK) name

This is sample output of the **show mka session detail** command:

```

Switch# show mka session detail
MKA Detailed Status for MKA Session
=====
Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI..... 0022.bdcf.9a01/0002
Interface MAC Address.... 0022.bdcf.9a01
MKA Port Identifier..... 2
Interface Name..... GigabitEthernet1/0/1
Audit Session ID..... 0B0B0B3D0000034F050FA69B
CAK Name (CKN)..... 46EFE9FE85199FE404FB7AFA3FD0732E
Member Identifier (MI)... D7B00EDA353242704CC6B0DB
Message Number (MN)..... 7
Authenticator..... YES
Key Server..... YES
Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D7B00EDA353242704CC6B0DB00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)
MKA Policy Name..... *DEFAULT POLICY*
Key Server Priority..... 0
Delay Protection..... NO
Replay Protection..... YES

```

```

Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Cipher Suite..... 0080020001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES
# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1
Live Peers List:
  MI                      MN                      Rx-SCI (Peer)
  -----
  DA296D3E62E0961234BF39A6 7                      001b.2140.ec4c/0000
Potential Peers List:
  MI                      MN                      Rx-SCI (Peer)
  -----

```

This is sample output of the **show mka session interface** command:

```

Switch# show mka session interface gigabitethernet1/0/25
Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/25.
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI          Key-Svr Status   CKN
=====
Gi1/0/25 001b.2140.ec3c/0000 replay-policy    0A05783B0000001700448BA8
2         001e.bdfe.6d99/0002 YES      Secured        3808F996026DFB8A2FCEC9A88BBD0680

```

Related Commands

Command	Description
clear mka sessions	Clears all MKA sessions or clear MKA sessions on a port-ID, interface, or Local TX-SCI.
macsec	Enables MACsec on an interface.

show mka statistics

To display global MACsec Key Agreement (MKA) Protocol statistics and error counters, use the **show mka statistics** command in privileged EXEC mode.

show mka statistics [**interface***interface-id***port-id***port-id*] | [**local-sci***sci*]

Syntax Description		
interface <i>interface-id</i>		(Optional) Displays statistics for an MKA session on an interface. Only physical interfaces are valid.
port-id <i>port-id</i>		Displays a summary of active MKA sessions running on the interface with the specified port ID. To see the port ID, enter the show mka session or show mka session interface interface-id command. Port identifier values begin at 2 and monotonically increase for each new active session using a virtual port on the same physical interface.
local-sci <i>sci</i>		(Optional) Shows statistics for an MKA session identified by its Local TX-SCI. To determine the Local TX-SCI for a session, enter the show mka session detail command. The SCI must be 8 octets (16 hexadecimal digits) long.
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

This is an example of the **show mka statistics** command output:

```
Switch# show mka statistics
MKA Global Statistics
=====
MKA Session Totals
  Secured..... 32
  Reauthentication Attempts.. 31
  Deleted (Secured)..... 1
  Keepalive Timeouts..... 0
CA Statistics
  Pairwise CAKs Derived..... 32
  Pairwise CAK Rekeys..... 31
  Group CAKs Generated..... 0
  Group CAKs Received..... 0
SA Statistics
  SAKs Generated..... 32
  SAKs Rekeyed..... 31
  SAKs Received..... 0
  SAK Responses Received..... 32
```

```

MKPDU Statistics
  MKPDUs Validated & Rx..... 580
    "Distributed SAK"..... 0
    "Distributed CAK"..... 0
  MKPDUs Transmitted..... 597
    "Distributed SAK"..... 32
    "Distributed CAK"..... 0
MKA Error Counter Totals
=====
Bring-up Failures..... 0
Reauthentication Failures..... 0
SAK Failures
  SAK Generation..... 0
  Hash Key Generation..... 0
  SAK Encryption/Wrap..... 0
  SAK Decryption/Unwrap..... 0
CA Failures
  Group CAK Generation..... 0
  Group CAK Encryption/Wrap..... 0
  Group CAK Decryption/Unwrap..... 0
  Pairwise CAK Derivation..... 0
  CKN Derivation..... 0
  ICK Derivation..... 0
  KEK Derivation..... 0
  Invalid Peer MACsec Capability.. 2
MACsec Failures
  Rx SC Creation..... 0
  Tx SC Creation..... 0
  Rx SA Installation..... 0
  Tx SA Installation..... 0
MKPDU Failures
  MKPDU Tx..... 0
  MKPDU Rx Validation..... 0
  MKPDU Rx Bad Peer MN..... 0
  MKPDU Rx Non-recent Peerlist MN.. 0

```

Table 45: Table 0-7 show mka Global Statistics Output Fields (continued)

Field	Description
Reauthentications	Reauthentications from 802.1x.
Pairwise CAKs Derived	Pairwise secure connectivity association keys (CAKs) derived through EAP authentication.
Pairwise CAK Rekeys	Pairwise CAK rekeys after reauthentication.
Group CAKs Generated	Generated group CAKs while acting as a key server in a group CA.
Group CAKs Received	Received group CAKs while acting as a nonkey server member in a group CA.
SAK Rekeys	Secure association key (SAK) rekeys that have been initiated as key servers or received as nonkey server members.
SAKs Generated	Generated SAKs while acting as a key server in any CA.

Field	Description
SAKs Received	Received SAKs while acting as a nonkey server member in any CA.
MPDUs Validated & Rx	MACsec Key Agreement Protocol Data Units (MPDUs) received and validated.
MPDUs Transmitted	Transmitted MPDUs.

Related Commands

Command	Description
clear mka statistics	Clears all MKA statistics or those on a specified interface port-ID or Local TX-SCI.

show mka summary

To display a summary of MACsec Key Agreement (MKA) sessions and global statistics, use the **show mka summary** command in privileged EXEC mode.

show mka summary

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

This is an example of the **show mka summary** command output:

```
Switch# show mka summary
Summary of All Currently Active MKA Sessions...
=====
Total MKA Sessions..... 1
  Initializing (Waiting for Peer)..... 0
  Pending (Waiting for Peer MACsec Reply)... 0
  Secured (Secured MKA Session with MACsec).. 1
  Reauthenticating MKA Sessions..... 0
Interface Peer-RxSCI Policy-Name Audit-Session-ID
Port-ID Local-TxSCI Key-Svr Status CKN
=====
Gi1/0/25 001b.2140.ec3c/0000 replay-policy 0A05783B0000001700448BA8
2 001e.bdfe.6d99/0002 YES Secured 3808F996026DFB8A2FCEC9A88BBD0680
MKA Global Statistics
=====
MKA Session Totals
Secured..... 36
Reauthentications..... 23
Deleted (Secured)..... 0
Keepalive Timeouts..... 4
MACsec SAK-Use Timeouts.. 0
CA Statistics
Pairwise CAKs Derived.... 33
Pairwise CAK Rekeys..... 23
Group CAKs Generated..... 0
Group CAKs Received..... 0
SA Statistics
SAKs Generated..... 61
SAKs Rekeyed..... 54
SAKs Received..... 0
SAK Responses Received... 59
MKPDU Statistics
MKPDUs Validated & Rx.... 75774
"Distributed SAK"..... 0
"Distributed CAK"..... 0
MKPDUs Transmitted..... 75049
"Distributed SAK"..... 96
```

```

"Distributed CAK"..... 0
MKA Error Counter Totals
=====
Internal Failures..... 0
Session Failures
Failed while Initializing..... 6
Failed while Pending MACsec... 2
Reauthentication Failure..... 0
SAK Failures
SAK Generation..... 0
Hash Key Generation..... 0
SAK Encryption/Wrap..... 0
SAK Decryption/Unwrap..... 0
CA Failures
Group CAK Generation..... 0
Group CAK Encryption/Wrap..... 0
Group CAK Decryption/Unwrap... 0
Pairwise CAK Derivation..... 0
CKN Derivation..... 0
ICK Derivation..... 0
KEK Derivation..... 0
MACsec Failures
Rx SC Creation..... 2
Tx SC Creation..... 2
Rx SA Installation..... 2
Tx SA Installation..... 0
MKPDU Failures
MKPDU Tx..... 0
MKPDU Rx Validation..... 13
Bad Peer MN (anti-replay).. 0
Non-recent Peerlist MN..... 0
MKA Policy Summary...
Policy KS Delay Replay Window Conf Interfaces
Name Priority Protect Protect Size Offset Applied
=====
*DEFAULT POLICY* 0 NO YES 0 0 Gi1/0/26 Gi1/0/29
replay-policy 0 NO YES 300 0 Gi1/0/25
Incredible-59#sh mka policy replay-policy
MKA Policy Summary...
Policy KS Delay Replay Window Conf Interfaces
Name Priority Protect Protect Size Offset Applied
=====
replay-policy 0 NO YES 300 0 Gi1/0/25

```

Table 46: Table 0-8 show mka summary Output Fields

Field	Description
Reauthentications	Reauthentications from 802.1x.
Pairwise CAKs Derived	Pairwise secure connectivity association keys (CAKs) derived through EAP authentication.
Pairwise CAK Rekeys	Pairwise CAK rekeys after reauthentication.
Group CAKs Generated	Generated group CAKs while acting as a key server in a group CA.
Group CAKs Received	Received group CAKs while acting as a nonkey server member in a group CA.

Field	Description
SAK Rekeys	Secure association key (SAK) rekeys that have been initiated as key servers or received as a non-key server members.
SAKs Generated	Generated SAKs while acting as a key server in any CA.
SAKs Received	Received SAKs while acting as a nonkey server member in any CA.
MPDUs Validated & Rx	MACsec Key Agreement Protocol Data Units (MPDUs) received and validated.
MPDUs Transmitted	Transmitted MPDUs.

Related Commands

Command	Description
show mka policy	Displays information about defined MKA protocol policies.
show mka session	Displays a summary of active MKA sessions.
show mka statistics	Displays global MKA statistics.

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:

```
Device# show radius server-group all
Server group radius
  Sharecount = 1  sg_unconfigured = FALSE
  Type = standard  Memlocks = 1
```

This table describes the significant fields shown in the display.

Table 47: 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.

```
Device> show storm-control
Interface Filter State Upper Lower Current
-----
Gi1/0/1 Forwarding 20 pps 10 pps 5 pps
Gi1/0/2 Forwarding 50.00% 40.00% 0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Device> show storm-control gigabitethernet 1/0/1
Interface Filter State Upper Lower Current
-----
Gi1/0/1 Forwarding 20 pps 10 pps 5 pps
```

The following table describes the fields in the show storm-control display:

Table 48: 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.

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:

```
Device# 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
```

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:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [{group-name vlan-group-name [user_count]]}
```

Syntax Description	
group-name <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	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If you enter the **group-name** keyword, only the members of the specified VLAN group are displayed.

This example shows how to display the members of a specified VLAN group:

```
Device# show vlan group group-name group2
vlan group group1 :40-45
```

This example shows how to display number of users in each of the VLANs in a group:

```
Device# show vlan group group-name group2 user_count
VLAN      : Count
-----
40         : 5
41         : 8
42         : 12
43         : 2
44         : 9
45         : 0
```


storm-control

To enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface, use the **storm-control** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

```
storm-control {action {shutdown | trap} | {broadcast | multicast | unicast} level {level [level-low] |
bps bps [bps-low] | pps pps [pps-low]}}
no storm-control {action {shutdown | trap} | {broadcast | multicast | unicast} level}
```

Syntax Description

action	Specifies the action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap.
shutdown	Disables the port during a storm.
trap	Sends an SNMP trap when a storm occurs.
broadcast	Enables broadcast storm control on the interface.
multicast	Enables multicast storm control on the interface.
unicast	Enables unicast storm control on the interface.
level	Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port.
<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 1000000000.0. 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:

```
Device(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Device(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Device(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Device(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the **switchport port-security aging** command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the **no** form of this command.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

Syntax Description	
static	Enables aging for statically configured secure addresses on this port.
time <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:

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# switchport port-security aging time 2  
Device(config-if)# switchport port-security aging type inactivity  
Device(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses:

```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# no switchport port-security aging static
```

switchport port-security mac-address

To configure secure MAC addresses or sticky MAC address learning, use the **switchport port-security mac-address** interface configuration command. To return to the default setting, use the **no** form of this command.

```
switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}]} | sticky
[{mac-address | vlan {vlan-id {access | voice}}]}]
```

Syntax Description

mac-address A secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured.

vlan vlan-id (Optional) On a trunk port only, specifies the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used.

vlan access (Optional) On an access port only, specifies the VLAN as an access VLAN.

vlan voice (Optional) On an access port only, specifies the VLAN as a voice VLAN.

Note The **voice** keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

sticky Enables the interface for sticky learning. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.

mac-address (Optional) A MAC address to specify a sticky secure MAC address.

Command Default

No secure MAC addresses are configured.
Sticky learning is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- You cannot configure static secure or sticky secure MAC addresses in the voice VLAN.
- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
- Voice VLAN is supported only on access ports and not on trunk ports.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky mac-address** interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.
- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky mac-address** interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode trunk
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport port-security mac-address sticky
Device(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Device(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

switchport port-security maximum

To configure the maximum number of secure MAC addresses, use the **switchport port-security maximum** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

```
switchport port-security maximum value [vlan [{vlan-list | [{access | voice}]}]]
no switchport port-security maximum value [vlan [{vlan-list | [{access | voice}]}]]
```

Syntax Description

value	Sets the maximum number of secure MAC addresses for the interface. The default setting is 1.
vlan	(Optional) For trunk ports, sets the maximum number of secure MAC addresses on a VLAN or range of VLANs. If the vlan keyword is not entered, the default value is used.
vlan-list	(Optional) Range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used.
access	(Optional) On an access port only, specifies the VLAN as an access VLAN.
voice	(Optional) On an access port only, specifies the VLAN as a voice VLAN.
Note	The voice keyword is available only if voice VLAN is configured on a port and if that port is not the access VLAN.

Command Default

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

The maximum number of secure MAC addresses that you can configure on a switch or switch stack is set by the maximum number of available MAC addresses allowed in the system. This number is determined by the active Switch Database Management (SDM) template. See the **sdm prefer** command. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

- When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to two. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but is not learned on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.

Voice VLAN is supported only on access ports and not on trunk ports.

- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Device(config)# interface gigabitethernet 2/0/2
Device(config-if)# switchport mode access
Device(config-if)# switchport port-security
Device(config-if)# switchport port-security maximum 5
```

switchport port-security violation

To configure secure MAC address violation mode or the action to be taken if port security is violated, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {protect | restrict | shutdown | shutdown vlan}
no switchport port-security violation {protect | restrict | shutdown | shutdown vlan}

Syntax Description		
	protect	Sets the security violation protect mode.
	restrict	Sets the security violation restrict mode.
	shutdown	Sets the security violation shutdown mode.
	shutdown vlan	Sets the security violation mode to per-VLAN shutdown.

Command Default The default violation mode is **shutdown**.

Command Modes Interface configuration

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

Usage Guidelines In the security violation protect mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.



Note We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit.

In the security violation restrict mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

In the security violation shutdown mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shutdown** interface configuration commands.

When the security violation mode is set to per-VLAN shutdown, only the VLAN on which the violation occurred is error-disabled.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port.
- A secure port cannot be a routed port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Gigabit or 10-Gigabit EtherChannel port group.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command. You can manually re-enable the port by entering the **shutdown** and **no shutdown** interface configuration commands or by using the **clear errdisable interface** privileged EXEC command.

You can verify your settings by using the **show port-security** privileged EXEC command.

This example show how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device(config)# interface gigabitethernet2/0/2  
Device(config)# switchport port-security violation shutdown vlan
```

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*
no tacacs server

Syntax Description	
name	Name of the private TACACS+ server host.

Command Default No TACACS+ server is configured.

Command Modes Global configuration (config)

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

Usage Guidelines The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples The following example shows how to configure the TACACS server using the name `server1` and enter TACACS+ server configuration mode to perform further configuration:

```
Device(config)# tacacs server server1
Device(config-server-tacacs)#
```

Related Commands	Command	Description
	address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
	key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
	port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
	send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
	single-connection (TACACS+)	Enables all TACACS packets to be sent to the same server using a single TCP connection.
	timeout (TACACS+)	Configures the time to wait for a reply from the specified TACACS server.

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:

```
Device(config)# ipv6 snooping policy policy1  
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
```

trusted-port

To configure a port to become a trusted port, use the **trusted-port** command in IPv6 snooping policy mode or ND inspection policy configuration mode. To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description This command has no arguments or keywords.

Command Default No ports are trusted.

Command Modes ND inspection policy configuration
 IPv6 snooping configuration

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

Usage Guidelines When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

This example shows how to define an NDP policy name as policy1, place the switch in NDP inspection policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
```

This example shows how to define an IPv6 snooping policy name as policy1, place the switch in IPv6 snooping policy configuration mode, and configure the port to be trusted:

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
```

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

<i>name</i>	Name of the VLAN map.
<i>number</i>	(Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

Command Default

There are no VLAN map entries and no VLAN maps applied to a VLAN.

Command Modes

Global configuration

Command History

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

Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**—Sets the action to be taken (forward or drop).
- **default**—Sets a command to its defaults.
- **exit**—Exits from VLAN access-map configuration mode.
- **match**—Sets the values to match (IP address or MAC address).
- **no**—Negates a command or set its defaults.

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map name [number]** command with a sequence number to delete a single entry.

Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs. For more information about VLAN map entries, see the software configuration guide for this release.

This example shows how to create a VLAN map named vac1 and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Device(config)# vlan access-map vac1  
Device(config-access-map)# match ip address acl1  
Device(config-access-map)# action forward
```

This example shows how to delete VLAN map vac1:

```
Device(config)# no vlan access-map vac1
```

vlan filter

To apply a VLAN map to one or more VLANs, use the **vlan filter** command in global configuration mode on the switch stack or on a standalone switch. To remove the map, use the **no** form of this command.

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```



Note

This command is not supported on switches running the LAN Base feature set.

Syntax Description

<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 tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094.
all	Adds the map to all VLANs.

Command Default

There are no VLAN filters.

Command Modes

Global configuration

Command History

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

Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

For more information about VLAN map entries, see the software configuration guide for this release.

This example applies VLAN map entry map1 to VLANs 20 and 30:

```
Device(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry mac1 from VLAN 20:

```
Device(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

Syntax Description

<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:

```
Device(config)# vlan group group1 vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device(config)# no vlan group group1 vlan-list 7
```




PART **XIII**

Stack Manager and High Availability

- [Stack Manager and High Availability, on page 839](#)



Stack Manager and High Availability

- [debug platform stack-manager](#), on page 840
- [main-cpu](#), on page 841
- [mode sso](#), on page 842
- [policy config-sync prc reload](#), on page 843
- [redundancy](#), on page 844
- [redundancy config-sync mismatched-commands](#), on page 845
- [redundancy force-switchover](#), on page 847
- [redundancy reload](#), on page 848
- [reload](#), on page 849
- [session](#), on page 851
- [show platform stack-manager](#), on page 852
- [show redundancy](#), on page 853
- [show redundancy config-sync](#), on page 857
- [show switch](#), on page 859
- [stack-mac persistent timer](#), on page 863
- [stack-mac update force](#), on page 864
- [standby console enable](#), on page 865
- [switch stack port](#), on page 866
- [switch priority](#), on page 867
- [switch provision](#), on page 868
- [switch renumber](#), on page 870

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
----------------------	--------------------------

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

Usage Guidelines	From the redundancy main configuration submode, use the standby console enable command to enable the standby switch.
-------------------------	---

This example shows how to enter the redundancy main configuration submode and enable the standby switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device#
```

mode sso

To set the redundancy mode to stateful switchover (SSO), use the **mode sso** command in redundancy configuration mode.

mode sso

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Redundancy configuration
----------------------	--------------------------

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

Usage Guidelines The **mode sso** command can be entered only from within redundancy configuration mode.

Follow these guidelines when configuring your system to SSO mode:

- You must use identical Cisco IOS images on the switches in the stack to support SSO mode. Redundancy may not work due to differences between the Cisco IOS releases.
- If you perform an online insertion and removal (OIR) of the module, the switch resets during the stateful switchover and the port states are restarted only if the module is in a transient state (any state other than Ready).
- The forwarding information base (FIB) tables are cleared on a switchover. Routed traffic is interrupted until route tables reconverge.

This example shows how to set the redundancy mode to SSO:

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)#
```

policy config-sync prc reload

To reload the standby switch if a parser return code (PRC) failure occurs during configuration synchronization, use the **policy config-sync reload** command in redundancy configuration mode. To specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs, use the **no** form of this command.

```
policy config-sync {bulk | lbl} prc reload
no policy config-sync {bulk | lbl} prc reload
```

Syntax Description	bulk Specifies bulk configuration mode.	
	lbl Specifies line-by-line (lbl) configuration mode.	
Command Default	The command is enabled by default.	
Command Modes	Redundancy configuration	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

This example shows how to specify that the standby switch is not reloaded if a parser return code (PRC) failure occurs during configuration synchronization:

```
Device(config-red) # no policy config-sync bulk prc reload
```

redundancy

To enter redundancy configuration mode, use the **redundancy** command in global configuration mode.

redundancy

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Global configuration
----------------------	----------------------

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

Usage Guidelines	The redundancy configuration mode is used to enter the main CPU submode, which is used to enable the standby switch.
-------------------------	--

To enter the main CPU submode, use the **main-cpu** command while in redundancy configuration mode.

From the main CPU submode, use the **standby console enable** command to enable the standby switch.

Use the **exit** command to exit redundancy configuration mode.

This example shows how to enter redundancy configuration mode:

```
Device (config) # redundancy
Device (config-red) #
```

This example shows how to enter the main CPU submode:

```
Device (config) # redundancy
Device (config-red) # main-cpu
Device (config-r-mc) #
```

redundancy config-sync mismatched-commands

To allow the standby switch to join the stack if a configuration mismatch occurs between the active and standby switches, use the **redundancy config-sync mismatched-commands** command in privileged EXEC mode.

redundancy config-sync {ignore | validate} mismatched-commands

Syntax Description	ignore	Ignores the mismatched command list.
	validate	Revalidates the mismatched command list with the modified running-configuration.
Command Default	None	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.2SE	This command was introduced.

Usage Guidelines If the command syntax check in the running configuration of the active switch fails while the standby switch is booting, use the **redundancy config-sync mismatched-commands** command to display the Mismatched Command List (MCL) on the active switch and to reboot the standby switch.

The following is a log entry example for mismatched commands:

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
! <submode> "interface"
- ip address 192.0.2.0 255.255.255.0
! </submode> "interface"
```

To display all mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the running configuration of the active switch.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby switch.

You can ignore the MCL by doing the following:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby switch; the system changes to SSO mode.



Note If you ignore the mismatched commands, the out-of-sync configuration at the active switch and the standby switch still exists.

3. Verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

If SSO mode cannot be established between the active and standby switches because of an incompatibility in the configuration file, a mismatched command list (MCL) is generated at the active switch and a reload into route processor redundancy (RPR) mode is forced for the standby switch.



Note RPR mode is supported on Catalyst 3850 switches as a fallback in case of errors. It is not configurable.

If you attempt to establish an SSO after removing the offending configuration and rebooting the standby switch with the same image, the C3K_REDUNDANCY-2-`IOS_VERSION_CHECK_FAIL` and ISSU-3-`PEER_IMAGE_INCOMPATIBLE` messages appear because the peer image is listed as incompatible. You can clear the peer image from the incompatible list with the **redundancy config-sync ignore mismatched-commands EXEC** command while the peer is in a standby cold (RPR) state. This action allows the standby switch to boot in a standby hot (SSO) state when it reloads.

This example shows how to revalidate the mismatched command list with the modified configuration:

```
Device# redundancy config-sync validate mismatched-commands
Device#
```

redundancy force-switchover

To force a switchover from the active switch to the standby switch, use the **redundancy force-switchover** command in privileged EXEC mode on a switch stack.

redundancy force-switchover

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	None
------------------------	------

Command Modes	Privileged EXEC
----------------------	-----------------

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

Usage Guidelines Use the **redundancy force-switchover** command to manually switch over to the redundant switch. The redundant switch becomes the new active switch that runs the Cisco IOS image, and the modules are reset to their default settings.

The old active switch reboots with the new image and joins the stack.

If you use the **redundancy force-switchover** command on the active switch, the switchports on the active switch go down.

If you use this command on a switch that is in a partial ring stack, the following warning message appears:

```
Device# redundancy force-switchover
Stack is in Half ring setup; Reloading a switch might cause stack split
This will reload the active unit and force switchover to standby[confirm]
```

This example shows how to manually switch over from the active to the standby supervisor engine:

```
Device# redundancy force-switchover
Device#
```

redundancy reload

To force a reload of one or all of the switches in the stack, use the **redundancy reload** command in privileged EXEC mode.

redundancy reload {peer | shelf}

Syntax Description	
peer	Reloads the peer unit.
shelf	Reboots all switches in the stack.

Command Default	None
-----------------	------

Command Modes	Privileged EXEC
---------------	-----------------

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

Usage Guidelines	Before using this command, see the “Performing a Software Upgrade” section of the <i>Stacking Configuration Guide (Catalyst 3850 Switches)</i> for additional information.
------------------	--

Use the **redundancy reload shelf** command to reboot all the switches in the stack.

This example shows how to manually reload all switches in the stack:

```
Device# redundancy reload shelf
Device#
```


reload

To reload the stack member and to apply a configuration change, use the **reload** command in privileged EXEC mode.

```
reload [{/noverify | /verify}] [{LINE | at | cancel | in | slot stack-member-number | standby-cpu}]
```

Syntax Description		
/noverify	(Optional)	Specifies to not verify the file signature before the reload.
/verify	(Optional)	Verifies the file signature before the reload.
<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:

```
Device# reload
System configuration has been modified. Save? [yes/no]: yes
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm] yes
```

This example shows how to reload a specific stack member:

```
Device# reload slot 6
Proceed with reload? [confirm] y
```

This example shows how to reload a single-switch switch stack (there is only one member switch):

```
Device# reload slot 3
System configuration has been modified. Save? [yes/no]: y
Proceed to reload the whole Stack? [confirm] y
```

session

To access the diagnostic shell of a specific stack member or to access the Cisco IOS prompt of the standby Device use the **session** command in privileged EXEC mode on the active Device.

```
session {standby ios | switch [stack-member-number]}
```

Syntax Description	standby ios	Accesses the Cisco IOS prompt of the standby Device.
		Note You cannot configure the standby Device using this command.
	switch	Accesses the diagnostic shell of a stack member.
	<i>stack-member-number</i>	(Optional) Stack member number to access from the active switch. The range is 1 to 9.

Command Default None

Command Modes Privileged EXEC

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

Usage Guidelines When you access the Cisco IOS prompt on the standby Device, `-stby` is appended to the system prompt. You cannot configure the standby Device at the `Device-stby>` prompt.

When you access the diagnostic shell of a stack member, `(diag)` is appended to the system prompt.

Examples

This example shows how to access stack member 3:

```
Device# session switch 3  
Device(diag)>
```

This example shows how to access the standby Device:

```
Device# session standby ios  
Device-stby>
```

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 857 .
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:

```
Device# show redundancy
Redundant System Information :
```

```

-----
    Available system uptime = 6 days, 9 hours, 23 minutes
Switchovers system experienced = 0
    Standby failures = 0
    Last switchover reason = not known

    Hardware Mode = Simplex
Configured Redundancy Mode = SSO
Operating Redundancy Mode = SSO
    Maintenance Mode = Disabled
    Communications = Down          Reason: Simplex mode

Current Processor Information :
-----
    Active Location = slot 1
    Current Software state = ACTIVE
    Uptime in current state = 6 days, 9 hours, 23 minutes
    Image Version = Cisco IOS Software, IOS-XE Software, Catalyst 3
850 L3 Switch Software (CAT3850-UNIVERSALK9-M), Version 03.08.59.EMD EARLY DEPLO
YMENT ENGINEERING NOVA_WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_11
05
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sun 16-S
    Configuration register = 0x102

Peer (slot: 0) information is not available because it is in 'DISABLED' state
Device#

```

This example shows how to display redundancy facility client information:

```

Device# show redundancy clients
Group ID = 1
clientID = 20002   clientSeq = 4   EICORE HA Client
clientID = 24100   clientSeq = 5   WCM_CAPWAP
clientID = 24101   clientSeq = 6   WCM_RRM HA
clientID = 24103   clientSeq = 8   WCM_QOS HA
clientID = 24105   clientSeq = 10  WCM_MOBILITY
clientID = 24106   clientSeq = 11  WCM_DOT1X
clientID = 24107   clientSeq = 12  WCM_APFROGUE
clientID = 24110   clientSeq = 15  WCM_CIDS
clientID = 24111   clientSeq = 16  WCM_NETFLOW
clientID = 24112   clientSeq = 17  WCM_MCAST
clientID = 24120   clientSeq = 18  wcm_comet
clientID = 24001   clientSeq = 21  Table Manager Client
clientID = 20010   clientSeq = 24  SNMP SA HA Client
clientID = 20007   clientSeq = 27  Installer HA Client
clientID = 29      clientSeq = 60  Redundancy Mode RF
clientID = 139     clientSeq = 61  IfIndex
clientID = 3300    clientSeq = 62  Persistent Variable
clientID = 25      clientSeq = 68  CHKPT RF
clientID = 20005   clientSeq = 74  IIF-shim
clientID = 10001   clientSeq = 82  QEMU Platform RF

```

<output truncated>

The output displays the following information:

- clientID displays the client's ID number.
- clientSeq displays the client's notification sequence number.
- Current redundancy facility state.

This example shows how to display the redundancy facility counter information:

```
Device# show redundancy counters
Redundancy Facility OMs

      comm link up = 0
      comm link down = 0
      invalid client tx = 0
      null tx by client = 0
      tx failures = 0
      tx msg length invalid = 0

      client not rxing msgs = 0
      rx peer msg routing errors = 0
      null peer msg rx = 0
      errored peer msg rx = 0

      buffers tx = 0
      tx buffers unavailable = 0
      buffers rx = 0
      buffer release errors = 0

      duplicate client registers = 0
      failed to register client = 0
      Invalid client syncs = 0
```

Device#

This example shows how to display redundancy facility history information:

```
Device# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM_QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_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:

```
Device# show redundancy slaves
Group ID = 1
Slave/Process ID = 6107 Slave Name = [installer]
Slave/Process ID = 6109 Slave Name = [eicored]
Slave/Process ID = 6128 Slave Name = [snmp_subagent]
Slave/Process ID = 8897 Slave Name = [wcm]
Slave/Process ID = 8898 Slave Name = [table_mgr]
Slave/Process ID = 8901 Slave Name = [iosd]
```

Device#

This example shows how to display information about the redundancy facility state:

```
Device# show redundancy states
my state = 13 -ACTIVE
peer state = 1 -DISABLED
Mode = Simplex
Unit ID = 1

Redundancy Mode (Operational) = SSO
Redundancy Mode (Configured) = SSO
Redundancy State = Non Redundant
Manual Swact = disabled (system is simplex (no peer unit))

Communications = Down Reason: Simplex mode

client count = 75
client_notification_TMR = 360000 milliseconds
keep_alive TMR = 9000 milliseconds
keep_alive count = 0
keep_alive threshold = 18
RF debug mask = 0
```

Device#

show redundancy config-sync

To display a configuration synchronization failure or the ignored mismatched command list (MCL), if any, use the **show redundancy config-sync** command in EXEC mode.

```
show redundancy config-sync {failures {bem | mcl | prc} | ignored failures mcl}
```

Syntax Description	failures	Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.
	bem	Displays a BEM failed command list, and forces the standby switch to reboot.
	mcl	Displays commands that exist in the switch's running configuration but are not supported by the image on the standby switch, and forces the standby switch to reboot.
	prc	Displays a PRC failed command list and forces the standby switch to reboot.
	ignored failures mcl	Displays the ignored MCL failures.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines When two versions of Cisco IOS images are involved, the command sets supported by two images might differ. If any of those mismatched commands are executed on the active switch, the standby switch might not recognize those commands, which causes a configuration mismatch condition. If the syntax check for the command fails on the standby switch during a bulk synchronization, the command is moved into the MCL and the standby switch is reset. To display all the mismatched commands, use the **show redundancy config-sync failures mcl** command.

To clean the MCL, follow these steps:

1. Remove all mismatched commands from the active switch's running configuration.
2. Revalidate the MCL with a modified running configuration by using the **redundancy config-sync validate mismatched-commands** command.
3. Reload the standby switch.

Alternatively, you could ignore the MCL by following these steps:

1. Enter the **redundancy config-sync ignore mismatched-commands** command.
2. Reload the standby switch; the system transitions to SSO mode.



Note If you ignore the mismatched commands, the out-of-synchronization configuration on the active switch and the standby switch still exists.

3. You can verify the ignored MCL with the **show redundancy config-sync ignored mcl** command.

Each command sets a return code in the action function that implements the command. This return code indicates whether or not the command successfully executes. The active switch maintains the PRC after executing a command. The standby switch executes the command and sends the PRC back to the active switch. A PRC failure occurs if these two PRCs do not match. If a PRC error occurs at the standby switch either during bulk synchronization or line-by-line (LBL) synchronization, the standby switch is reset. To display all PRC failures, use the **show redundancy config-sync failures prc** command.

To display best effort method (BEM) errors, use the **show redundancy config-sync failures bem** command.

This example shows how to display the BEM failures:

```
Device> show redundancy config-sync failures bem
BEM Failed Command List
-----

The list is Empty
```

This example shows how to display the MCL failures:

```
Device> show redundancy config-sync failures mcl
Mismatched Command List
-----

The list is Empty
```

This example shows how to display the PRC failures:

```
Device# show redundancy config-sync failures prc
PRC Failed Command List
-----

The list is Empty
```

show switch

To display information that is related to the stack member or the switch stack, use the **show switch** command in EXEC mode.

```
show switch [{stack-member-number | detail | neighbors | stack-ports [{summary}]]
```

Syntax Description	
<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:

```
Device# 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:

```
Device# 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:

```
Device# show switch 6
```

Switch#	Role	Mac Address	Priority	State
6	Member	0003.e31a.1e00	1	Ready

This example shows how to display the neighbor information for a stack:

```
Device# show switch neighbors
Switch #      Port A      Port B
```

```

-----
      6      None      8
      8      6      None

```

This example shows how to display stack-port information:

```

Device# show switch stack-ports
Switch #   Port A   Port B
-----
      6     Down     Ok
      8     Ok      Down

```

This example shows the output for the `show switch stack-ports summary` command. The table that follows describes the fields in the display.

```

Device# show switch stack-ports summary
Switch#/  Stack  Neighbor  Cable  Link  Link  Sync  #  In
Port#     Port  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 49: 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.

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	0 (Optional) Continues using the MAC address of the current active switch indefinitely, even after a new active switch takes over.				
	<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.				
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:

```
Device(config)# stack-mac persistent timer
```

You can verify your settings by entering the **show running-config** privileged EXEC command. If enabled, **stack-mac persistent timer** is shown in the output.

stack-mac update force

To update the stack MAC address to the MAC address of the active switch, use the **stack-mac update force** command in EXEC mode on the active switch.

stack-mac update force

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes User EXEC
Privileged EXEC

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

Usage Guidelines By default, the stack MAC address is not changed to the MAC address of the new active switch during a high availability (HA) failover. Use the **stack-mac update force** command to force the stack MAC address to change to the MAC address of the new active switch.

If the switch with the same MAC address as the stack MAC address is currently a member of the stack, the **stack-mac update force** command has no effect. (It does not change the stack MAC address to the MAC address of the active switch.)



Note If you do not change the stack MAC address, Layer 3 interface flapping does not occur. It also means that a foreign MAC address (a MAC address that does not belong to any of the switches in the stack) could be the stack MAC address. If the switch with this foreign MAC address joins another stack as the active switch, two stacks will have the same stack MAC address. You must use the **stack-mac update force** command to resolve the conflict.

This example shows how to update the stack MAC address to the MAC address of the active switch:

```
Device> stack-mac update force
Device>
```

You can verify your settings by entering the **show switch** privileged EXEC command. The stack MAC address includes whether the MAC address is local or foreign.

standby console enable

To enable access to the standby console switch, use the **standby console enable** command in redundancy main configuration submode. To disable access to the standby console switch, use the **no** form of this command.

standby console enable
no standby console enable

Syntax Description This command has no arguments or keywords.

Command Default Access to the standby console switch is disabled.

Command Modes Redundancy main configuration submode

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

Usage Guidelines This command is used to collect and review specific data about the standby console. The command is useful primarily for Cisco technical support representatives troubleshooting the switch.

This example shows how to enter the redundancy main configuration submode and enable access to the standby console switch:

```
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)#
```

switch stack port

To disable or enable the specified stack port on the member, use the **switch** command in privileged EXEC mode on a stack member.

switch *stack-member-number* **stack port** *port-number* {**disable** | **enable**}

Syntax Description

<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:

```
Device# switch 4 stack port 2 disable
```

switch priority

To change the stack member priority value, use the **switch priority** command in EXEC mode on the active switch.

```
switch stack-member-number priority new-priority-value
```

Syntax Description

stack-member-number Current stack member number. The range is 1 to 9.

new-priority-value New stack member priority value. The range is 1 to 15.

Command Default

The default priority value is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

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

Usage Guidelines

The new priority value is a factor when a new active switch is elected. When you change the priority value the active switch is not changed immediately.

Examples

This example shows how to change the priority value of stack member 6 to 8:

```
Device# switch 6 priority 8
Changing the Switch Priority of Switch Number 6 to 8
Do you want to continue?[confirm]
```

switch provision

To supply a configuration to a new switch before it joins the switch stack, use the **switch provision** command in global configuration mode on the active switch. To delete all configuration information that is associated with the removed switch (a stack member that has left the stack), use the **no** form of this command.

switch *stack-member-number* **provision** *type*
no switch *stack-member-number* **provision**

Syntax Description	<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.

```
Device(config)# switch 2 provision WS-xxxx
Device(config)# end
```

```
Device# show running-config | include switch 2
!
interface GigabitEthernet2/0/1
!
interface GigabitEthernet2/0/2
!
interface GigabitEthernet2/0/3
<output truncated>
```

You also can enter the **show switch** user EXEC command to display the provisioning status of the switch stack.

This example shows how to delete all configuration information about stack member 5 when the switch is removed from the stack:

```
Device(config)# no switch 5 provision
```

You can verify that the provisioned switch is added to or removed from the running configuration by entering the **show running-config** privileged EXEC command.

switch renumber

To change the stack member number, use the **switch renumber** command in EXEC mode on the active switch.

switch *current-stack-member-number* **renumber** *new-stack-member-number*

Syntax Description

current-stack-member-number Current stack member number. The range is 1 to 9.

new-stack-member-number New stack member number for the stack member. The range is 1 to 9.

Command Default

The default stack member number is 1.

Command Modes

User EXEC

Privileged EXEC

Command History

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

Usage Guidelines

If another stack member is already using the member number that you just specified, the active switch assigns the lowest available number when you reload the stack member.



Note

If you change the number of a stack member, and no configuration is associated with the new stack member number, that stack member loses its current configuration and resets to its default configuration.

Do not use the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* command on a provisioned switch. If you do, the command is rejected.

Use the **reload slot** *current stack member number* privileged EXEC command to reload the stack member and to apply this configuration change.

Examples

This example shows how to change the member number of stack member 6 to 7:

```
Device# switch 6 renumber 7
WARNING:Changing the switch number may result in a configuration change for that switch.
The interface configuration associated with the old switch number will remain as a provisioned
configuration.
Do you want to continue?[confirm]
```



PART **XIV**

System Management

- [Autonomic Networking](#) , on page 873
- [System Management Commands](#), on page 889
- [Tracing](#) , on page 987



Autonomic Networking

- [autonomic adjacency-discovery, on page 874](#)
- [autonomic connect, on page 875](#)
- [clear autonomic, on page 876](#)
- [debug autonomic, on page 878](#)
- [show autonomic control-plane, on page 879](#)
- [show autonomic device, on page 881](#)
- [show autonomic interfaces, on page 882](#)
- [show autonomic intent, on page 884](#)
- [show autonomic l2-channels, on page 885](#)
- [show autonomic service, on page 886](#)
- [show autonomic neighbor, on page 887](#)

autonomic adjacency-discovery

To enable adjacency discovery (neighbor discovery) on an interface, use the **autonomic adjacency-discovery** command in interface configuration mode. To disable adjacency discovery, use the **no** form of this command.

autonomic adjacency-discovery
no autonomic adjacency-discovery

Command Default Adjacency discovery is not enabled.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples To enable adjacency discovery:

```
Device(config)# interface Tunnel100
Device(config-if)# autonomic adjacency-discovery
```

autonomic connect

To connect a non autonomic device to autonomic domain use the **autonomic connect** command in interface configuration mode. To disconnect a device from the domain, use the **no** form of this command.

autonomic connect
no autonomic connect

Command Default Device is not connected to the domain.

Command Modes Interface configuration (config-if)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines You need to configure **no switchport** on the interface before configuring the **autonomic connect** command.

Examples To connect a non autonomic device to autonomic domain :

```
Device > enable
Device# configure terminal
Device(config)# int gig 1/0/1
Device(config-if)# no switchport
Device(config-if)# autonomic connect
Device(config-if)# ipv6 address 5000::1/64
```

clear autonomic

To clear or reset autonomic information, use the **clear autonomic** command in privileged EXEC configuration mode.

clear autonomic {**device** | **neighbor** *neighbor's UDI* | **registrar accepted-device** *device UDI*}

Syntax Description	device	Clears or resets device information.
	neighbor <i>udi</i>	Clears or resets neighbor information.
	registrar accepted-device <i>udi</i>	Clears public key stored for each enrolled device

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines The **clear autonomic device** command clears or resets all device-specific autonomic information, including the information obtained in the bootstrapping process. The **clear autonomic neighbor** command clears the neighbor-related information learned during the neighbor discovery. If no neighbor is specified, the command clears the entire neighbor database. The **clear registrar accepted-device** clears the public key stored for each device enrolled by the registrar.

Examples

To clear all device-specific autonomic information:

```
Device #clear autonomic device

% invoke syslog_an_delete_host: vrf cisco_autonomic
discriminator
Device#
Jul 15 05:55:53.987: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:53.988: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:55:53.990: %AN-6-ACP_DIKE_TO_NBR_REMOVED: Removed DIKE on ACP Tunnel100000 from
Device (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) to Neighbor (Addr
FD08:2EEF:C2EE:0:E865:493B:ACFB:5) connected on interface GigabitEthernet1/0/3
Jul 15 05:55:54.006: %AN-6-ACP_CHANNEL_TO_NBR_REMOVED: Removed ACP Tunnel100000 from Device
(Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) to Neighbor (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:5)
connected on interface GigabitEthernet1/0/3
Jul 15 05:55:54.015: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:54.016: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100000, changed
state to down
Jul 15 05:55:54.097: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:55:54.104: %AN-5-NBR_LOST: Device with ACP (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7)
lost connectivity to its Neighbor (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:5) on interface
GigabitEthernet1/0/3
Jul 15 05:55:54.113: %AN-5-CD_STATE_CHANGED: L2 Channel (0) Removed - Our Intf
(GigabitEthernet1/0/3), Nbr UDI (PID:WS-C3850-24U SN:FCW1934D05Z), Nbr Intf
(GigabitEthernet1/0/3)
Jul 15 05:55:56.004: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel100000, changed
```

```

state to down
Jul 15 05:55:56.005: %LINK-5-CHANGED: Interface Tunnell100000, changed state to
administratively down
Jul 15 05:56:04.128: %AN-6-UDI_AVAILABLE: UDI - PID:WS-C3650-24TD SN:FDO1942E1YK
Jul 15 05:56:36.306: %AN-5-CD_STATE_CHANGED: L2 Channel (0) Created - Our Intf
(GigabitEthernet1/0/3), Nbr UDI (PID:WS-C3850-24U SN:FCW1934D05Z), Nbr Intf
(GigabitEthernet1/0/3)
Jul 15 05:56:36.310: %LINK-3-UPDOWN: Interface ANI1, changed state to up
Jul 15 05:56:37.294: %LINEPROTO-5-UPDOWN: Line protocol on Interface ANI1, changed state
to up
Jul 15 05:56:44.138: %AN-5-NBR_ADDED: Device with UDI (PID:WS-C3850-24U SN:FCW1934D05Z) is
added as a Neighbor to Device with (Addr UNKNOWN) on the interface GigabitEthernet1/0/3
Jul 15 05:56:44.146: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.148: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.150: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.247: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.258: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:56:44.269: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:04.897: %CRYPTO-6-AUTOGEN: Generated new 3072 bit key pair
Jul 15 05:57:05.359: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.815: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:05.817: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.830: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:05.840: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:05.841: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.308: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:06.311: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.313: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.314: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.810: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.811: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:06.811: %AN-5-DEVICE_BOOTSTRAPPED_BY_ANR: Device with UDI (PID:WS-C3650-24TD
SN:FDO1942E1YK) and (Addr FD08:2EEF:C2EE:0:E865:493B:ACFB:7) has been boot trapped by
autonomic registrar, in autonomic domain cisco.com
Jul 15 05:57:06.815: %AN-6-ACP_VRF_GLOBAL_CREATE_SUCCESS: Device UDI (PID:WS-C3650-24TD
SN:FDO1942E1YK) Autonomic VRF created globally vrf name cisco_autonomic, vrf id 3
Jul 15 05:57:06.823: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback100000, changed
state to up
Jul 15 05:57:06.828: %AN-6-ACP_VRF_INTERFACE_CREATE_SUCCESS: Device UDI (PID:WS-C3650-24TD
SN:FDO1942E1YK) Autonomic VRF created successfully on interface Loopback100000, vrf name
cisco_autonomic, vrf id 3
Jul 15 05:57:06.837: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.840: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.842: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:06.842: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:07.905: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnell100001, changed
state to up
Jul 15 05:57:08.159: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: (NOT ERROR BUT WARNING ONLY) ID
of FE80::3A20:56FF:FEF3:7158 (type 5) and certificate addr with
Jul 15 05:57:08.160: %CRYPTO-6-IKMP_NO_ID_CERT_ADDR_MATCH: (NOT ERROR BUT WARNING ONLY) ID
of FE80::3A20:56FF:FEF3:7158 (type 5) and certificate addr with
Jul 15 05:57:11.959: %SYS-5-CONFIG_I: Configured from console by console
Jul 15 05:57:11.960: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write
memory" to save new IOS PKI configuration
Jul 15 05:57:11.963: %SYS-5-CONFIG_I: Configured from console by console

```

debug autonomic

To enable debugging of autonomic information, use the **debug autonomic** command in privileged EXEC mode. To stop the debugging, use the **no** form of this command.

```
debug autonomic {Bootstrap | Channel-Discovery | Infra | Intent | Neighbor-Discovery | Registrar |
Services} {aaa | all | database | events | ntp | packets} {info | moderate | severe}
no debug autonomic {Bootstrap | Channel-Discovery | Infra | Intent | Neighbor-Discovery | Registrar |
Services} {aaa | all | database | events | ntp | packets} {info | moderate | severe}
```

Syntax Description		
bootstrap		Enables debugging of bootstrapping information.
Channel-Discovery		Enables debugging of channel discovery information.
Infra		Enables debugging of infra information.
Intent		Enables debugging of intent information.
Neighbor-Discovery		Enables debugging of neighbor information.
Registrar		Enables debugging of registrar information.
Services		Enables debugging of autonomic services information.
aaa		Enables debugging authentication, authorization, and accounting information.
all		Enables all debugging.
events		Provides information about autonomic events.
ntp		Enables debugging of Network Time Protocol (NTP) information.
packets		Provides information about autonomic packets.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Use this command to debug the autonomic networking information.

show autonomic control-plane

To display information about the autonomic control plane, use the **show autonomic control-plane** command in privileged EXEC mode.

show autonomic control-plane [{detail}]

Syntax Description	detail (Optional) Displays detailed information.
--------------------	--

Command Modes	Privileged EXEC (#)
---------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

To display information about the autonomic control plane:

```
Device# show autonomic control-plane

VRF Name                cisco_autonomic
Device Address          FD08:2EEF:C2EE:0:E865:493B:ACFB:7
RPL                    floating-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:5

Neighbor                ACP                Channel ACP Security
-----
PID:WS-C3850-24U SN:FCW1934D05Z  Tunnel100002  DIKE
```

To display information about the autonomic control plane in detail:

```
Device# show autonomic control-plane detail

VRF Name                cisco_autonomic
Device Address          FD08:2EEF:C2EE:0:E865:493B:ACFB:7
RPL                    grounded-node, Dag-id = FD08:2EEF:C2EE:0:E865:493B:ACFB:1

Neighbor: PID:WS-C3850-24U SN:FCW1934D05Z
Uptime(Created Time): 00:12:16 ( 2016-07-15 05:38:53 UTC)
Supported ACP Channel: IPv6 GRE Tunnel
Negotiated ACP Channel: IPv6 GRE Tunnel
Tunnel Name Tunnel100000
Tunnel Source Interface ANI1
Tunnel Source FE80::5AAC:78FF:FE09:F383
Tunnel Destination FE80::3A20:56FF:FEF3:7158
Supported ACP Security: IPSec, DIKE
Negotiated ACP Security: DIKE
```

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

Table 50: show autonomic control-plane Field Descriptions

Field	Description
VRF Name	VPN routing and forwarding (VRF) name.
Device Address	IPv6 address.

Field	Description
RPL	RPL node details.
Neighbor	Unique Device Identifier (UDI) of the neighbor.
Tunnel Name	Tunnel name.
Tunnel Source Interface	IP address of the source tunnel interface.
Tunnel Source	IP address of the tunnel source.
Tunnel Destination	IP address of the destination.

show autonomic device

To display the autonomic device information, use the **show autonomic device** command in privileged EXEC mode.

show autonomic device

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

To display the autonomic device information:

```
Device# show autonomic device

      Status                               Enabled
      Type                                 Autonomic Node
      UDI                                  PID:WS-C3650-24TD SN:FDO1942E1YK
      Device ID                             e865.493b.acfb-7
      Domain ID                             cisco.com
      Domain Certificate                     (sub:) ou=cisco.com+serialNumber=PID:WS-C3650-24TD
SN:FDO1942E1YK,cn=e865.493b.acfb-7
      Certificate Serial Number              09
      Device Address                         FD08:2EEF:C2EE:0:E865:493B:ACFB:7
      Domain Cert is Valid
```

show autonomic interfaces

To display information about the autonomic interfaces, use the **show autonomic interfaces** command in privileged EXEC mode.

show autonomic interfaces

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

To display information about the autonomic interfaces:

```
Device# show autonomic interfaces
```

Interface	Channel Disc	AD Enabled	Intf Type
GigabitEthernet0/0	None	No	L2 untagged If
GigabitEthernet1/0/1	None	No	L2 untagged If
GigabitEthernet1/0/2	None	No	L2 untagged If
GigabitEthernet1/0/3	Probing	No	L2 untagged If
GigabitEthernet1/0/4	None	No	L2 untagged If
GigabitEthernet1/0/5	None	No	L2 untagged If
GigabitEthernet1/0/6	None	No	L2 untagged If
GigabitEthernet1/0/7	None	No	L2 untagged If
GigabitEthernet1/0/8	None	No	L2 untagged If
GigabitEthernet1/0/9	None	No	L2 untagged If
GigabitEthernet1/0/10	None	No	L2 untagged If
GigabitEthernet1/0/11	None	No	L2 untagged If
GigabitEthernet1/0/12	None	No	L2 untagged If
GigabitEthernet1/0/13	None	No	L2 untagged If
GigabitEthernet1/0/14	None	No	L2 untagged If
GigabitEthernet1/0/15	None	No	L2 untagged If
GigabitEthernet1/0/16	None	No	L2 untagged If
GigabitEthernet1/0/17	None	No	L2 untagged If
GigabitEthernet1/0/18	None	No	L2 untagged If
GigabitEthernet1/0/19	None	No	L2 untagged If
GigabitEthernet1/0/20	None	No	L2 untagged If
GigabitEthernet1/0/21	None	No	L2 untagged If
GigabitEthernet1/0/22	None	No	L2 untagged If
GigabitEthernet1/0/23	None	No	L2 untagged If
GigabitEthernet1/0/24	None	No	L2 untagged If
GigabitEthernet1/1/1	None	No	L2 untagged If
GigabitEthernet1/1/2	None	No	L2 untagged If
TenGigabitEthernet1/1/3	None	No	L2 untagged If
TenGigabitEthernet1/1/4	None	No	L2 untagged If
Vlan1	None	No	Virtual If
AN11	None	Yes	Virtual If
Loopback100000	None	No	Virtual If
Tunnel100002	None	No	Virtual If

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

Table 51: show autonomic interface Field Descriptions

Field	Description
Interface	Interface name.
Channel Disc	Channel discovery.
AD Enabled	

show autonomic intent

To verify the configured intent range, use the **show autonomic intent** command in privileged EXEC mode.

show autonomic intent

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Usage Guidelines Intent is automatically sent to all nodes in an autonomic domain. So, every node should show the same intent

Examples To display information about the configured intent range:

```
Device# show autonomic intent

Intent File : Available
Version Num : 1443520505 (Parsed)
Version Time: 2015-09-29 09:55:05 UTC
Outer Vlans : 30-35,40,45
Outer Vlans count : 8
```

show autonomic l2-channels

To display the results of Channel Discovery, use the **show autonomic l2-channels** command in privileged EXEC mode.

show autonomic l2-channels

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

To display the results of Channel Discovery:

```
Device# show autonomic l2-channels
```

```
AN L2 Channel Discovery Info :
```

```
Nbr UDI                               Encap    Our Intf    State    Retry
```

```
-----
```

```
PID:WS-C3850-24U SN:FCW1934D05Z  4018    Gi1/0/3    Active  1
```

To display more detailed information:

```
Device# show autonomic l2-channels detail
```

```
AN L2 Channel Discovery Info :
```

```
-----
```

```
Nbr UDI                               : PID:WS-C3850-24U SN:FCW1934D05Z
ANI Intf                               : ANI1
Encap                                   : 0
Nbr Intf                               : GigabitEthernet1/0/3
Our Intf                               : GigabitEthernet1/0/3
Keepalives Missed                      : 0
Channel Status                         : Active
```

show autonomic service

To verify the service announcements distributed over the Autonomic Control Plane (ACP) to all devices, use the **show autonomic service** command in privileged EXEC mode.

show autonomic service

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

To display information about the services:

```
Device# show autonomic service

Service          IP-Addr
Syslog           5000::100
AAA              5000::100
  AAA Accounting Port 1813
  AAA Authorization Port 1812
Autonomic registrar FD08:2EEF:C2EE:0:E865:493B:ACFB:1
  ANR type          IOS CA
Config Server Address 5000::100
Auto IP Server     UNKNOWN
```

show autonomic neighbor

To display information about autonomic neighbors, use the **show autonomic neighbor** command in privileged EXEC mode.

show autonomic neighbor [{detail}]

Syntax Description	detail (Optional) Displays detailed information.
---------------------------	---

Command Modes	Privileged EXEC (#)
----------------------	---------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.3.1	This command was introduced.

Examples

The following is sample output from the **show autonomic neighbor** command:

```
Device# show autonomic neighbor
UDI                               Device-ID           Domain             Interface
-----
PID:WS-C3850-24U SN:FCW1934D05Z  e865.493b.acfb-5   cisco.com         ANI1
```

The following is sample output from the **show autonomic neighbor detail** command:

```
Device# show autonomic neighbor detail
UDI: "PID:WS-C3850-24U SN:FCW1934D05Z"

      Device ID           e865.493b.acfb-5
      Domain ID           cisco.com
      Address              FD08:2EEF:C2EE:0:E865:493B:ACFB:5
      State                Nbr inside the Domain
      Credential           Domain Cert
      Credential Validation Passed
      Last Validated Time  2016-07-15 05:48:37 UTC
      Certificate Expiry Date 2017-07-15 05:30:39 UTC
      Certificate Expire Countdown 31534693 (secs)
      Number of Links connected 1

      Link:
      Local Interface:     ANI2
      Remote Interface:    ANI2
      IP Address:          FE80::3A20:56FF:FEF3:7158
      Uptime(Discovered Time): 00:14:21 ( 2016-07-15 05:38:05 UTC)
      Last Refreshed time: 0 seconds ago
```

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

Table 52: show autonomic neighbor detail Field Descriptions

Field	Description
UDI	Unique device identifier.

Field	Description
Device Identifier	Device name.
Domain Identifier	Domain name.
State	Information about whether the neighbor is inside or outside the domain. If a device is inside an autonomic domain, it must have a valid domain certificate.
Credential	Detection method.
Credential Validation	Detection validation.
Number of Links connected	Number of neighbors detected.
Local Interface	Interface from which the neighbor is connected.
Remote Interface	Interface to which the neighbor is connected.
IP Address	IPv6 address of the neighbor,



System Management Commands

- [arp](#), on page 891
- [boot](#), on page 892
- [cat](#), on page 893
- [clear location](#), on page 894
- [clear location statistics](#), on page 895
- [copy](#), on page 896
- [copy startup-config tftp:](#), on page 897
- [copy tftp: startup-config](#), on page 898
- [debug voice diagnostics mac-address](#), on page 899
- [delete](#), on page 900
- [dir](#), on page 901
- [emergency-install](#), on page 903
- [exit](#), on page 905
- [flash_init](#), on page 906
- [help](#), on page 907
- [l2 traceroute](#), on page 908
- [license right-to-use](#), on page 909
- [location](#), on page 911
- [location plm calibrating](#), on page 914
- [mac address-table move update](#), on page 915
- [mgmt_init](#), on page 916
- [mkdir](#), on page 917
- [more](#), on page 918
- [no debug all](#), on page 919
- [rename](#), on page 920
- [request platform software console attach switch](#), on page 921
- [request platform software package clean](#), on page 923
- [request platform software package copy](#), on page 925
- [request platform software package describe file](#), on page 926
- [request platform software package expand](#), on page 932
- [request platform software package install auto-upgrade](#), on page 934
- [request platform software package install commit](#), on page 935
- [request platform software package install file](#), on page 936

- request platform software package install rollback, on page 939
- request platform software package install snapshot, on page 941
- request platform software package verify, on page 943
- request platform software package uninstall, on page 944
- reset, on page 945
- rmdir, on page 946
- sdm prefer, on page 947
- set, on page 948
- show avc client, on page 951
- show cable-diagnostics tdr, on page 952
- show debug, on page 954
- show env, on page 955
- show env xps, on page 957
- show flow monitor, on page 961
- show license right-to-use, on page 966
- show location, on page 968
- show mac address-table move update, on page 969
- show platform integrity, on page 970
- show platform sudi certificate, on page 971
- show sdm prefer, on page 973
- system env temperature threshold yellow, on page 975
- test cable-diagnostics tdr, on page 977
- traceroute mac, on page 978
- traceroute mac ip, on page 981
- type, on page 983
- unset, on page 984
- version, on page 986

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:
-----------------	--

```
Device: arp 172.20.136.8  
arp'ing 172.20.136.8...  
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

```
boot [-post | -n | -p | flag] filesystem:/file-url...
```

Syntax Description	
-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
-n	(Optional) Pause for the Cisco IOS Debugger immediately after launching.
-p	(Optional) Pause for the JTAG Debugger right after loading the image.
<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 device attempts to automatically boot the system by using the information in the BOOT environment variable, if any.

If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you specify boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session.

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin  
Device: boot
```

After entering this command, you are prompted to start the setup program.

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem: Specifies a file system.

/file-url Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

clear location

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags information in the entire database, use the **clear location** command in EXEC mode.

clear location [**mac-address** *mac-address* | **rfid**]

Syntax Description

mac-address <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:

```
Device> clear location rfid
```

clear location statistics

To clear radio-frequency identification (RFID) statistics, use the **clear location statistics** command in EXEC mode.

clear location statistics

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User EXEC
Privileged EXEC

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

The following is sample output from the **clear location rfid** command and shows how to clear RFID statistics:

```
Device> clear location statistics
```

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:

```
Device: copy usbflash0:test1.text usbflash0:test4.text  
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir filesystem:** boot loader command.

copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

copy startup-config tftp: *remote host {ip-address}/{name}*

Syntax Description	<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	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:

```
Device: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

copy tftp: startup-config *remote host {ip-address}/{name}*

Syntax Description	<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:

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug voice diagnostics mac-address *mac-address1* **verbose** **mac-address** *mac-address2* **verbose**
nodebug voice diagnostics mac-address *mac-address1* **verbose** **mac-address** *mac-address2* **verbose**

Syntax Description	voice diagnostics	Configures voice debugging for voice clients.
	mac-address <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:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem:/file-url...*

Syntax Description

filesystem: Alias for a file system. Use **usbflash0**: for USB memory sticks.

/file-url... Path (directory) and filename to delete. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0**: boot loader command.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description

filesystem: Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.

/file-url (Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot Loader

Privileged EXEC

Command History

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

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
Device: dir flash:
Directory of flash:/
  2  -rwx      561   Mar 01 2013 00:48:15  express_setup.debug
  3  -rwx    2160256  Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
  4  -rwx      1048  Mar 01 2013 00:01:39  multiple-fs
  6  drwx      512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx      512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx      4316  Mar 01 2013 01:14:05  config.text
648 -rwx        5   Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

Table 53: 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.

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. After you perform the emergency install operation, run the boot flash:packages.conf command manually in boot loader mode, to boot the system.				

Example

This example shows how to perform the emergency install operation using the contents of an image file:

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....done
Nova Bundle Image
-----
Kernel Address      : 0x6042d5c8
Kernel Size        : 0x317ccc/3243212
Initramfs Address  : 0x60745294
Initramfs Size     : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range \
[0x80180000, 0x90000000].
#####
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)

Initiating Emergency Installation of bundle \
tftp:<url>
```

```

Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd

```

```

Booting...(use DDR clock 667 MHz)Initializing and Testing RAM
+++@@@###...++@@+@@+@@+@@+@@+@@+@@+@@+@@+@@done.
Memory Test Pass!

```

```

Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

```

```

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

```

```

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

```

```

boot

```


exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

exit

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Privileged EXEC
Global configuration

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

This example shows how to exit the configuration mode:

```
Device(config)# exit  
Device#
```

flash_init

To initialize the flash: file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Command Default

The flash: file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

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

Usage Guidelines

During the normal boot process, the flash: file system is automatically initialized.

Use this command to manually initialize the flash: file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot loader
----------------------	-------------

Command History	Release	Modification
		Cisco IOS XE 3.2SE

Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

I2 traceroute

To enable the Layer 2 traceroute server, use the **I2 traceroute** command in global configuration mode. Use the **no** form of this command to disable the Layer 2 traceroute server.

I2 traceroute
no I2 traceroute

Syntax Description This command has no arguments or keywords.

Command Modes Global configuration (config#)

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

Usage Guidelines Layer 2 traceroute is enabled by default and opens a listening socket on User Datagram Protocol (UDP) port 2228. To close the UDP port 2228 and disable Layer 2 traceroute, use the **no I2 traceroute** command in global configuration mode.

The following example shows how to configure Layer 2 traceroute using the **I2 traceroute** command.

```
Device# configure terminal
Device(config)# I2 traceroute
```

license right-to-use

To configure right-to-use access point adder licenses on the device, use the **license right-to-use** command in privileged EXEC mode.

license right-to-use {**activate** | **deactivate**} **apcount** | **ibase** | **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.
ibase <i>count</i>		Activates ibase 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:

```
Device# license right-to-use activate apcount evaluation
Device# end
```

This example shows how to activate an ap-count permanent license:

```
Device# license right-to-use deactivate apcount evaluation
Device# end
```

This example shows how to add a new ap-count license:

```
Device# license right-to-use activate apcount 500 slot 1
Device# end
```

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

```
location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location {admin-tag string | civic-location identifier {hostid} | civic-location identifier {hostid} |
elin-location {string | identifier id} | geo-location identifier {hostid} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

Syntax Description		
admin-tag	<i>string</i>	Configures administrative tag or site information. Site or location information in alphanumeric format.
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).
geo-location		Configures geo-spatial location information.
prefer		Sets location information source priority.

Command Default No default behavior or values.

Command Modes Global configuration

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

Usage Guidelines After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code**—Sets an additional civic location code.
- **additional-location-information**—Sets additional civic location information.
- **branch-road-name**—Sets the branch road name.
- **building**—Sets building information.
- **city**—Sets the city name.
- **country**—Sets the two-letter ISO 3166 country code.
- **county**—Sets the county name.
- **default**—Sets a command to its defaults.
- **division**—Sets the city division name.
- **exit**—Exits from the civic location configuration mode.
- **floor**—Sets the floor number.
- **landmark**—Sets landmark information.
- **leading-street-dir**—Sets the leading street direction.
- **name**—Sets the resident name.
- **neighborhood**—Sets neighborhood information.
- **no**—Negates the specified civic location data and sets the default value.
- **number**—Sets the street number.
- **post-office-box**—Sets the post office box.
- **postal-code**—Sets the postal code.
- **postal-community-name**—Sets the postal community name.
- **primary-road-name**—Sets the primary road name.
- **road-section**—Sets the road section.
- **room**—Sets room information.
- **seat**—Sets seat information.
- **state**—Sets the state name.
- **street-group**—Sets the street group.
- **street-name-postmodifier**—Sets the street name postmodifier.
- **street-name-premodifier**—Sets the street name premodifier.
- **street-number-suffix**—Sets the street number suffix.
- **street-suffix**—Sets the street suffix.
- **sub-branch-road-name**—Sets the sub-branch road name.
- **trailing-street-suffix**—Sets the trailing street suffix.
- **type-of-place**—Sets the type of place.
- **unit**—Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude**—Sets altitude information in units of floor, meters, or feet.
- **latitude**—Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.

- **longitude**—Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**—Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**—Sets the geographical location to its default attribute.
- **exit**—Exits from geographical location configuration mode.
- **no**—Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

This example shows how to configure civic location information on the switch:

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the switch:

```
Device(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the switch:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command in global configuration mode.

location plm calibrating {**multiband** | **uniband**}

Syntax Description

multiband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
uniband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

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:

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update receive
Device(config)# end
```

You can verify your setting by entering the **show mac address-table move update** privileged EXEC command.

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init** command in boot loader mode.

mgmt_init

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Boot loader

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

Usage Guidelines Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description	<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:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem: Alias for a file system. Use **flash:** for the system board flash device.

/file-url... Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

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.

```
Device: no debug all  
All possible debugging has been turned off.
```

rename

To rename a file, use the **rename** command in boot loader mode.

```
rename filesystem:/source-file-url filesystem:/destination-file-url
```

Syntax Description	
<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*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir filesystem:** boot loader command.

request platform software console attach switch

To start a session on a member switch, use the **request platform software console attach switch** command in privileged EXEC mode.



Note On stacking switches (Catalyst 3650/3850/9300/9500 switches), this command can only be used to start a session on the standby console. You cannot start a session on member switches. By default, all consoles are already active, so a request to start a session on the active console will result in an error.

request platform software console attach switch { *switch-number* | **active** | **standby** } { **0/0** | **R0** }

Syntax Description

switch-number Specifies the switch number. The range is from 1 to 9.

active Specifies the active switch.

standby Specifies the standby switch.

0/0 Specifies that the SPA-Inter-Processor slot is 0, and bay is 0.

Note Do not use this option with stacking switches. It will result in an error.

R0 Specifies that the Route-Processor slot is 0.

Command Default

By default, all switches in the stack are active.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

To start a session on the standby switch, you must first enable it in the configuration.

Examples

This example shows how to session to the standby switch:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
```

```
Device-stby> enable
Device-stby#
```

request platform software package clean

To remove media files that are not required, use the **request platform software package clean** command in privileged EXEC mode.

```
request platform software package clean [{file URL | pattern URL | switch switch-ID {file URL | pattern URL }]
```

Syntax Description	file <i>URL</i>	(Optional) Specifies the URL to the file. The URL contains the file system, directories, and the filename.
	pattern <i>URL</i>	(Optional) Specifies the pattern to clean one or more matching paths.
	switch <i>switch-ID</i>	(Optional) Specifies the switch for provisioning.

Command Default No default behavior or values

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to clean unused media files from the device:

```
Device# request platform software package clean
```

```
This operation may take several minutes...
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path consolidated:packages.conf
Cleaning sw/isos
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-guestshell.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpbase.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
  packages.conf
```

```
File is in use, will not delete.  
done.
```

```
SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package copy

To copy a Cisco IOS XE image file, use the **request platform software package copy** command in privileged EXEC mode.

request platform software package copy switch *switch-ID* **file** *file-URL* **to** *file-URL*

Syntax Description

switch <i>switch-ID</i>	Specifies the switch for provisioning.
file <i>file-URL</i>	URL to the consolidated package or sub-package.
to	Specifies the destination URL to where the files are to be copied.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to copy an image file to a destination directory:

```
Device# request platform software package copy switch all file
tftp://10.10.11.250/cat3k_caa-universalk9.16.08.05.SPA.bin to
ftp:cat3k_caa-universalk9.16.08.05.SPA.bin
```

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package describe file

To gather descriptive information about an individual module or a Cisco IOS-XE image file, use the **request platform software package describe file** command in privileged EXEC or diagnostic mode.

request platform software package describe file *URL* [**detail**] [**verbose**]

Syntax Description

<i>URL</i>	Specifies the URL to the file. The <i>URL</i> contains the file system, directories, and the filename.
detail	(Optional) Specifies detailed output.
verbose	(Optional) Displays verbose information, meaning that all information about the file is displayed on the console.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command can only be used to gather information on individual module and Cisco IOS-XE image files. Using this command to collect information on any other file will generate output, but the generated output is useless.

The output of this command can be used for the following functions:

- To confirm the individual module files that are part of a Cisco IOS-XE image.
- To confirm whether or not a file is bootable.
- To confirm the contexts in which a file must be reloaded or booted.
- To confirm whether or not a file is corrupted.
- To confirm file and header sizes, build dates, and various other general information.

Examples

In the following example, this command is entered to gather information about an individual SIP Base module file on the bootflash: file system.

```
Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
Size: 36954316
Timestamp: 2018-11-07 15:36:27 UTC
Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Raw disk-file SHA1sum:
3ee37cdbe276316968866b16df7d8a5733a1502e
```

```

Computed SHA1sum:
  f2db80416a1245a5b1abf2988088860b38ce7898
Contained SHA1sum:
  f2db80416a1245a5b1abf2988088860b38ce7898
Hashes match. Package is valid.

Header size:      204 bytes
Package type:     10000
Package flags:    0
Header version:   0

Internal package information:
Name: cc
BuildTime: 2018-11-07_05.24
ReleaseDate: Wed 07-Nov-18 01:00
RouteProcessor: rpl
Platform: Cat3XXX
User: mcpre
PackageName: ipbasek9
Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

```

Package is bootable on SIP when specified by packages provisioning file.

In the following example, this command is used to gather information about a Cisco IOS-XE image on the bootflash: file system.

```

Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
Size: 218783948
Timestamp: 2018-11-07 17:14:09 UTC
Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Raw disk-file SHA1sum:
  d2999fc7e27e01344903a42ffacd62c156eba4cc

Computed SHA1sum:
  5f8cda8518d01d8282d80ecd34f7715783f4a813
Contained SHA1sum:
  5f8cda8518d01d8282d80ecd34f7715783f4a813
Hashes match. Package is valid.

Header size:      204 bytes
Package type:     30000
Package flags:    0
Header version:   0

Internal package information:
Name: rp_super
BuildTime: 2018-11-07_05.24
ReleaseDate: Wed 07-Nov-18 01:00
RouteProcessor: rpl
Platform: Cat3XXX
User: mcpre
PackageName: ipbasek9
Build: cat3k_caa-universalk9_universalk9.16.09.02

Package is bootable from media and tftp.
Package contents:

```

```
Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
Size: 52072652
Timestamp: 2018-11-07 13:33:13 UTC

Raw disk-file SHA1sum:
  flaad6d687256aa327a4efa84deab949fbed12b8

Computed SHA1sum:
  15502fd1b8f9ffd4af4014ad4d8026c837929fe6
Contained SHA1sum:
  15502fd1b8f9ffd4af4014ad4d8026c837929fe6
Hashes match. Package is valid.

Header size:      204 bytes
Package type:     20000
Package flags:    0
Header version:   0

Internal package information:
  Name: fp
  BuildTime: 2018-11-07_05.24
  ReleaseDate: Wed 07-Nov-18 01:00
  RouteProcessor: rp1
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package is bootable on ESP when specified
by packages provisioning file.

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
Size: 21844172
Timestamp: 2018-11-07 13:33:01 UTC

Raw disk-file SHA1sum:
  025e6159dd91cef9d254ca9fff2602d8ce065939

Computed SHA1sum:
  ealb358324ba5815b9ea623b453a98800eae1c78
Contained SHA1sum:
  ealb358324ba5815b9ea623b453a98800eae1c78
Hashes match. Package is valid.

Header size:      204 bytes
Package type:     30004
Package flags:    0
Header version:   0

Internal package information:
  Name: ipbasek9
  BuildTime: 2018-11-07_05.24
  ReleaseDate: Wed 07-Nov-07 01:00
  RouteProcessor: rp1
  Platform: Cat3XXXX
  User: mcpre
  PackageName: ipbasek9
  Build: 16.9.20180925:160127

Package is not bootable.
```



```
Package: cat3k_caa-universalk9.16.09.02.SPA.bin
Size: 21520588
Timestamp: 2007-12-04 13:33:06 UTC
```

```
Raw disk-file SHA1sum:
  432dfa61736d8a51baefbb2d70199d712618dcd2
```

```
Computed SHA1sum:
  83c0335a3adcea574bff237a6c8640a110a045d4
```

```
Contained SHA1sum:
  83c0335a3adcea574bff237a6c8640a110a045d4
```

```
Hashes match. Package is valid.
```

```
Header size:      204 bytes
Package type:     30001
Package flags:    0
Header version:   0
```

```
Internal package information:
```

```
Name: rp_base
BuildTime: 2007-12-04_05.24
ReleaseDate: Tue 04-Dec-07 01:00
RouteProcessor: rp1
Platform: Cat3XXX
User: mcpre
PackageName: ipbasek9
Build: v_16.9.20180925:160127
```

```
Package is bootable on RP when specified
by packages provisioning file.
```

```
Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
Size: 24965324
Timestamp: 2018-11-07 13:33:08 UTC
```

```
Raw disk-file SHA1sum:
  eb964b33d4959c21b605d0989e7151cd73488a8f
```

```
Computed SHA1sum:
  19b58886f97c79f885ab76c1695d1a6f4348674e
```

```
Contained SHA1sum:
  19b58886f97c79f885ab76c1695d1a6f4348674e
```

```
Hashes match. Package is valid.
```

```
Header size:      204 bytes
Package type:     30002
Package flags:    0
Header version:   0
```

```
Internal package information:
```

```
Name: rp_daemons
BuildTime: 2018-11-07_05.24
ReleaseDate: Wed 07-Nov-07 01:00
RouteProcessor: rp1
Platform: Cat3XXX
User: mcpre
PackageName: ipbasek9
Build: v_16.9.20180925:160127
```

```
Package is not bootable.
```

```
Package: cat3k_caa-universalk9.16.09.02.SPA.bin
```

```

Size: 48515276
Timestamp: 2007-12-04 13:33:13 UTC

Raw disk-file SHA1sum:
  bc13462d6a4af7a817a7346a44a0ef7270e3a81b

Computed SHA1sum:
  f1235d703cc422e53bce850c032ff3363b587d70
Contained SHA1sum:
  f1235d703cc422e53bce850c032ff3363b587d70
Hashes match. Package is valid.

```

```

Header size:      204 bytes
Package type:     30003
Package flags:    0
Header version:   0

```

```

Internal package information:
  Name: rp_losd
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rpl
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127

```

Package is not bootable.

```

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
Size: 36954316
Timestamp: 2007-12-04 13:33:11 UTC

```

```

Raw disk-file SHA1sum:
  3ee37cdbe276316968866b16df7d8a5733a1502e

Computed SHA1sum:
  f2db80416a1245a5b1abf2988088860b38ce7898
Contained SHA1sum:
  f2db80416a1245a5b1abf2988088860b38ce7898
Hashes match. Package is valid.

```

```

Header size:      204 bytes
Package type:     10000
Package flags:    0
Header version:   0

```

```

Internal package information:
  Name: cc
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rpl
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127

```

Package is bootable on SIP when specified
by packages provisioning file.

```

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
Size: 19933388

```

```

Timestamp: 2007-12-04 13:33:06 UTC

Raw disk-file SHA1sum:
  44b6d15cba31fb0e9b27464665ee8a24b92adfd2

Computed SHA1sum:
  b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
Contained SHA1sum:
  b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
Hashes match. Package is valid.

Header size:      204 bytes
Package type:     10001
Package flags:    0
Header version:   0

Internal package information:
  Name: cc_spa
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127

Package is not bootable.

```

Related Commands

Command	Description
request platform software package install file	Upgrades an individual package or a superpackage file.

request platform software package expand

To extract the individual modules from a Cisco IOS-XE image, use the **request platform software package expand** command in privileged EXEC mode.

request platform software package expand {file *source-URL* | switch *switch-ID* file *source-URL*}[
to *destination-URL*] [**auto-copy**] [**force**] [**overwrite**] [**retain-source-file**] [**verbose**] [**wipe**]

Syntax Description

<i>source-URL</i>	Specifies the URL to the Cisco IOS-XE file that stores the contents that will be extracted.
switch <i>switch-ID</i>	Specifies the switch ID.
to <i>destination-URL</i>	(Optional) Specifies the destination URL where the files that were extracted from the Cisco IOS-XE file are left after the operation is complete. If this option is not entered, the Cisco IOS-XE image file contents are extracted onto the same directory where the Cisco IOS-XE image file is currently stored.
auto-copy	(Optional) Copies packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
over-write	(Optional) Overwrites non-identical packages and unused provisioning files.
retain-to-source	(Optional) Retains the source file after expansion.
verbose	(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.
wipe	(Optional) Erases all content on the destination snapshot directory before extracting the files and placing them on the snapshot directory.

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command only extracts individual module files and a provisioning file from the Cisco IOS-XE image. Additional configuration is needed to configure the router to boot using the provisioning files and run using the individual modules.

When this command is used, copies of each module and the provisioning file within the Cisco IOS-XE image are copied and placed on the destination directory. The Cisco IOS-XE image file is unchanged after the operation is complete.

If the **to destination-URL** option is not entered, the Cisco IOS-XE image contents will be extracted onto the same directory where the Cisco IOS-XE image is currently stored.

If this command is used to extract individual module files onto a directory that already contains individual module files, the files are extracted to an automatically created directory on the destination device.

Examples

The following example shows how to extract individual modules and the provisioning file from a Cisco IOS-XE image that has already been placed in the directory where the user wants to store the individual modules and the provisioning file.

Output of the directory before and after the extraction is given to confirm that files were extracted.

```
Device# dir bootflash:

Directory of bootflash:/
 11  drwx          16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401 drwx           4096   Dec 4 2018 11:27:41 +00:00  .installer
 12  -rw-       218783948   Dec 4 2018 12:12:16 +00:00  cat3k_caa-universalk9.16.09.02.SPA.bin

Device# request platform software package expand file
bootflash:cat3k_caa-universalk9.16.09.02.SPA.bin

Verifying parameters
Validating package type
Copying package files

Device# dir bootflash:

Directory of bootflash:/
 11  drwx          16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401 drwx           4096   Dec 4 2018 11:27:41 +00:00  .installer
 12  -rw-       218783948   Dec 4 2018 12:12:16 +00:00  cat3k_caa-universalk9.16.09.02.SPA.bin
28802 -rw-           7145   Dec 4 2018 12:14:22 +00:00  packages.conf
928833536 bytes total (483700736 bytes free)
```

Related Commands

Command	Description
request platform software package install file	Upgrades an individual module or a Cisco IOS-XE file.

request platform software package install auto-upgrade

To initiate automatic upgrade of software on all incompatible switches, use the **request platform software package install auto-upgrade** command in privileged EXEC mode.

request platform software package install auto-upgrade

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 Denali 16.1.1	This command was introduced.

Examples

The following example shows how to automatically upgrade the software:

```
Device# request platform software package install auto-upgrade
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package install commit

To cancel the rollback timer and commit a software upgrade, use the **request platform software package install commit** command in privileged EXEC mode.

```
request platform software package install switch switch-ID commit [verbose]
```

Syntax Description

switch <i>switch-ID</i>	Specifies the switch ID.
verbose	(Optional) Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

This command is entered after the **request platform software package install switch** *switch-ID* **file auto-rollback** command is used to begin an individual sub-package or a consolidated package upgrade. When the **auto-rollback** *minutes* option is used, a rollback timer that cancels the upgrade after the number of specified *minutes* cancels the upgrade if the **request platform software package install switch** *switch-ID* **commit** command is not entered to commit the upgrade.

The rollback timer expires and the upgrade does not complete; and the device continues running the previous sub-package or consolidated package.

Examples

The following example shows how to commit an upgrade:

```
Device# request platform software package install switch all commit
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package install file

To upgrade a consolidated package or an individual sub-package, use the **request platform software package install file** command in privileged EXEC mode.

request platform software package install switch *switch-ID* **file** *file-URL* [**auto-rollback** *minutes*] [**interface-module-delay** *seconds*] [**provisioning-file** *provisioning-file-URL*] [**slot** *slot-number*] [**bay** *bay-number*] [**auto-copy**] [**force**] [**ignore-compact-check**] [**mdr**] [**new**] [**on-reboot**] [**retain-source-file**] [**verbose**]

Syntax Description

switch <i>switch-ID</i>	Specifies the switch for provisioning.
<i>file-URL</i>	URL to the consolidated package or sub-package.
auto-rollback <i>minutes</i>	(Optional) Specifies the setting of a rollback timer, and sets the number of minutes on the rollback timer before the rollback timer expires.
interface-module-delay <i>seconds</i>	(Optional) Specifies the interface module restart timeout delay.
provisioning-file <i>provisioning-file-URL</i>	(Optional) Specifies the URL to the provisioning file. A provisioning file is used for booting only when a device is booted using individual sub-packages.
slot <i>slot-number</i>	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.
bay <i>bay-number</i>	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
ignore-compact-check	(Optional) Specifies that the compatibility check is ignored.
mdr	(Optional) Specifies that minimal disruptive restart is used.
new	(Optional) Creates a new package provisioning file.
on-reboot	(Optional) Specifies that the installation will not be completed until the next RP reboot.
retain-source-file	(Optional) Retains the source file after installation.
verbose	(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.

Command Default

If you do not enter the **request platform software package install file** command, the consolidated or sub package upgrades are not initiated on the device.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines This command is used to upgrade consolidated packages and individual sub-packages.

When the **auto-rollback** *minutes* option is used, the **request platform software package install switch** *switch-ID* **commit** command must be entered before the rollback timer expires to complete the upgrade. If this command is not entered, the device rolls back to the previous software version. The rollback timer expires after the number of specified *minutes*. If the **auto-rollback** *minutes* option is not used, the upgrade automatically happens.

In the following example, the **request platform software package install** command is used to upgrade a consolidated package. The **force** option, which forces the upgrade past any prompt (such as, already having the same consolidated package installed), is used in this example.

```
Device# request platform software package install rp 0 file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

WARNING:
WARNING: Candidate software will be installed upon reboot
WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
```

```

Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned. New software will load on reboot.

```

Device# **reload**



Note A reload must be performed to finish this procedure.

Related Commands

Command	Description
request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
request platform software package install rollback	Rolls back a previous software upgrade.
request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

request platform software package install rollback

To roll back a previous software upgrade, use the **request platform software package install rollback** command in privileged EXEC mode.

```
request platform software package install switch switch-ID rollback [{as-booted | provisioning-file
provisioning-file-URL}] [auto-copy] [force] [ignore-compact-check] [new] [on-reboot]
[retain-source-file] [verbose]
```

Syntax Description		
switch <i>switch-ID</i>		Specifies the switch for provisioning.
as-booted		(Optional) Specifies that the software update will not occur, and that the device will instead boot using the same procedure that it used during the last reboot.
provisioning-file <i>provisioning-file-URL</i>		(Optional) Specifies that the software update will not occur, and that the device will instead boot using the specified provisioning file.
auto-copy		(Optional) Specifies that the device will automatically copy packages to provisioning directory.
force		(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
ignore-compact-check		(Optional) Specifies that the compatibility check is ignored.
new		(Optional) Creates a new package provisioning file.
on-reboot		(Optional) Specifies that the installation will not be completed until the next reboot.
retain-source-file		(Optional) Retains the source file after installation,
verbose		(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.

Command Default No default behavior or values

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.1.1	This command was introduced.

Usage Guidelines This command rolls back a configuration that has an active rollback timer. Active rollback timers are used when the **auto-rollback** option is entered when software is being upgraded using the **request platform software package install file** command.

Examples

The following example shows that an upgrade using a rollback timer is rolled back to the previous configuration:

```
Device# request platform software package install switch all rollback
```

Related Commands

Command	Description
request platform software package install commit	Cancel the rollback timer and commits a software upgrade.
request platform software package install file	Upgrades a consolidated package or an individual sub-package.

request platform software package install snapshot

To create a snapshot directory that contains all the files extracted from a consolidated package, use the **request platform software package install snapshot** command in privileged EXEC mode.

request platform software package install switch *switch-ID* **snapshot to** *URL* [**as** *snapshot-provisioning-filename*] [**force**] [**verbose**] [**wipe**]

Syntax Description		
switch <i>switch-ID</i>		Specifies the switch for provisioning.
snapshot to <i>URL</i>		Creates a directory and extracts all files from the consolidated package into that directory. The directory is named in the command-line as part of the <i>URL_FS</i> . If the <i>URL_FS</i> is specified as a file system, the files in the consolidated package will be extracted onto the file system and not a directory on the file system.
as <i>snapshot-provisioning-filename</i>		(Optional) Renames the provisioning file in the snapshot directory. If this option is not used, the existing provisioning filename of the provisioning file in the consolidated package is used.
wipe		(Optional) Erases all content on the destination snapshot directory before extracting files and placing them on the snapshot directory.
force		(Optional) Specifies that the operation will be forced; meaning that the upgrade will proceed despite any warning messages.
verbose		(Optional) Displays verbose information, meaning all output is displayed on the console during the provisioning process.

Command Default No default behavior or values

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.1.1	This command was introduced.

Usage Guidelines This command is used to create a directory at the destination device and extract the individual sub-packages in a consolidated package to that directory.

The **request platform software package expand** command is the only other command that can be used to extract individual sub-packages from a consolidated package.

Examples

In the following example, a snapshot directory named `snapdir1_snap` is created in the bootflash: file system, and the individual sub-package files from the consolidated package are extracted into the snapshot directory.

The second portion of the example first sets up the router to reboot using the files in the snapshot directory (deletes all previous boot system commands, configures the configuration register, then enters a boot system command to boot using the extracted provisioning file), saves the new configuration, then reboots so the device will boot using the extracted provisioning file, which allows the router to run using the extracted individual sub-package files.

```
Device# request platform software package install switch all snapshot to
bootflash:snapdir1_snap

--- Starting active image file snapshot --- Validating snapshot parameters Creating
destination directory
Copying files to destination media
  Copied provisioning file as packages.conf
Moving files into final location Finished active image file snapshot
Device(config)# no boot system
Device(config)# config-register 0x1
Device(config)# boot system harddisk:snapdir1_snap/packages.conf
Device(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Device# write memory

Building configuration...
[OK]

Device# reload
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or an individual sub-package.

request platform software package verify

To verify the In-Service Software Upgrade (ISSU) software package compatibility, use the **requestplatform software package verify** command in privileged EXEC mode.

```
request platform software package verify switch switch-ID file file-URL [bay bay-number] [slot slot-number] [auto-copy] [force] [mdr]
```

Syntax Description

switch <i>switch-ID</i>	Specifies the switch for provisioning.
<i>file-URL</i>	URL to the consolidated package or sub-package.
bay <i>bay-number</i>	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
slot <i>slot-number</i>	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.
auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
mdr	(Optional) Specifies that minimal disruptive restart is used.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

The following example shows how to verify Cisco IOS XE image:

```
Device# request platform software package verify switch all file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin
```

Related Commands

Command	Description
request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
request platform software package install rollback	Rolls back a previous software upgrade.
request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

request platform software package uninstall

To uninstall a software package, use the **request platform software package uninstall** command in privileged EXEC mode.

request platform software package uninstall **switch** *switch-ID* **file** *file-URL* [**bay** *bay-number*] [**slot** *slot-number*] [**auto-copy**] [**force**] [**mdr**]

Syntax Description

switch <i>switch-ID</i>	Specifies the switch for provisioning.
<i>file-URL</i>	URL to the consolidated package or sub-package.
bay <i>bay-number</i>	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
slot <i>slot-number</i>	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.
auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
mdr	(Optional) Specifies that minimal disruptive restart is used.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

The following example shows how to uninstall a software package:

```
Device# request platform software package uninstall
```

Related Commands

Command	Description
request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
request platform software package install rollback	Rolls back a previous software upgrade.
request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

reset

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Boot loader
----------------------	-------------

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

Examples

This example shows how to reset the system:

```
Device: reset  
Are you sure you want to reset the system (y/n)? y  
System resetting...
```

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem: Alias for a file system. Use **usbflash0:** for USB memory sticks.

/directory-url... Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all of the files in the directory.

The device prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir filesystem:** boot loader command.

sdm prefer

To specify the SDM template for use on the switch, use the **sdm prefer** command in global configuration mode.

```
sdm prefer
{ advanced }
```

Syntax Description	advanced Supports advanced features such as NetFlow.
---------------------------	---

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Global configuration
----------------------	----------------------

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

Usage Guidelines In a device stack, all stack members must use the same SDM template that is stored on the active device. When a new device is added to a stack, the SDM configuration that is stored on the active device overrides the template configured on an individual device.

Example

This example shows how to configure the advanced template:

```
Device(config)# sdm prefer advanced
Device(config)# exit
Device# reload
```

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

set *variable value*

Syntax Description

<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 device 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 device from the boot loader mode.</p> <hr/> <p>BOOT <i>filesystem:/file-url</i>—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> <hr/> <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> <hr/> <p>HELPER <i>filesystem:/file-url</i>—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> <hr/> <p>PS1 <i>prompt</i>—Specifies a string that is used as the command-line prompt in boot loader mode.</p> <hr/> <p>CONFIG_FILE flash: <i>/file-url</i>—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p> <hr/> <p>BAUD <i>rate</i>—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> <hr/> <p>SWITCH_NUMBER <i>stack-member-number</i>—Changes the member number of a stack member.</p> <hr/> <p>SWITCH_PRIORITY <i>priority-number</i>—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 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1



Note Environment variables that have values are stored in the flash: file system in various files. Each line in the files contains an environment variable name and an equal sign followed by the value of the variable.

A variable has no value if it is not listed in these files; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “”) is a variable with a value.

Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash: file system.

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system filesystem: /file-url** global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper filesystem: /file-url** global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash: /file-url** global configuration command.

The SWITCH_NUMBER environment variable can also be set by using the **switch current-stack-member-number renumber new-stack-member-number** global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

```
show avc client client-mac top n application [aggregate | upstream | downstream]
```

Syntax Description

client *client-mac* Specifies the client MAC address.

top n application Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

The following is sample output from the **show avc client** command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate
```

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	7343	449860	61	94
2	unknown	99	13631	137	3
3	dhcp	18	8752	486	2
4	http	18	3264	181	1
5	tftp	9	534	59	0
6	dns	2	224	112	0

Last Interval (90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	9	540	60	100

show 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 device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
TDR test last run on: March 01 00:04:08
Interface  Speed  Local pair  Pair length          Remote pair  Pair status
-----
Gi1/0/23  1000M  Pair A      1 +/- 1 meters      Pair A      Normal
          Pair B      1 +/- 1 meters      Pair B      Normal
          Pair C      1 +/- 1 meters      Pair C      Normal
          Pair D      1 +/- 1 meters      Pair D      Normal
```

Table 54: Field Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.

Field	Description
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: <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:

```
Device# show interface gigabitethernet1/0/2
gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
% TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

show debug

show debug condition *Condition identifier* | *All conditions*

Syntax Description	<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:

```
Device# show debug condition all
```

To disable debugging, use the **no debug all** command.

show env

To display fan, temperature, and power information for the switch (standalone switch, stack master, or stack member), use the **show env** command in EXEC modes.

```
show env { all | fan | power [all | switch [switch-number]] | stack [stack-number] |
temperature [status] }
```

Syntax Description		
all		Displays fan, temperature and power environmental status.
fan		Displays the switch fan status.
power		Displays the power supply status.
all		(Optional) Displays the status for all power supplies.
switch <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.

Examples

This example shows how to display information about stack member 1 from the master switch:

```
Device> show env stack 1
Device 1:
Device Fan 1 is OK
Device Fan 2 is OK
Device Fan 3 is OK
FAN-PS1 is OK
```

```
FAN-PS2 is NOT PRESENT
Device 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius
```

```
Device>
```

This example shows how to display temperature value, state, and threshold values:

```
Device> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius
```

```
Device>
```

Table 55: 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 env xps

To display budgeting, configuration, power, and system power information for the Cisco eXpandable Power System (XPS) 2200, use the **show env xps** command in privileged EXEC mode.

```
show env xps { budgeting | configuration | port [ all | number ] | power | system |
thermal | upgrade | version }
```

Syntax Description		
budgeting		Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.
configuration		Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the show env xps configuration command to retrieve the non-default configuration.
port [all number]		Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9.
power		Displays the status of the XPS power supplies.
system		Displays the XPS system status.
thermal		Displays the XPS thermal status.
upgrade		Displays the XPS upgrade status.
version		Displays the XPS version details.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(55)SE1	This command was introduced.

Usage Guidelines Use the **show env xps** privileged EXEC command to display the information for XPS 2200.

Examples

This is an example of output from the show env xps budgeting command:

```
Switch#
=====

XPS 0101.0100.0000 :
=====
Data          Current   Power    Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
-----
223          1543
----- 1 - - 715 SP-PS
```

```

2      -      -      -      SP-PS      223      223
3      -      -      -      -          -          -
4      -      -      -      -          -          -
5      -      -      -      -          -          -
6      -      -      -      -          -          -
7      -      -      -      -          -          -
8      -      -      -      -          -          -
9      1      1100 -      RPS-NB      223      070
XPS   -      -      1100 -      -          -          -

```

This is an example of output from the show env xps configuration command:

```

Switch# show env xps configuration
=====
XPS 0101.0100.0000 :
=====
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4

```

This is an example of output from the show env xps port all command:

```

Switch#
XPS 010

-----
Port name           : -
Connected           : Yes
Mode                : Enabled (On)
Priority            : 1
Data stack switch # : - Configured role      : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
-----
Port name           : -
Connected           : Yes
Mode                : Enabled (On)
Priority            : 2
Data stack switch # : - Configured role      : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
-----
Port name           : -
Connected           : No
Mode                : Enabled (On)
Priority            : 3
Data stack switch # : - Configured role      : Auto-SP Run mode           : -
Cable faults        :
<output truncated>

```

This is an example of output from the show env xps power command:

```

=====
XPS 0101.0100.0000 :
=====
Port-Supply SW PID          Serial#    Status    Mode Watts
-----
XPS-A                Not present
XPS-B                NG3K-PWR-1100WAC  LIT13320NTV OK          SP   1100
1-A                  -          -          -          -

```

```

1-B      - -      -      -      SP      715
2-A      - -      -      -
2-B      - -      -      -
9-A      - -      100WAC  LIT141307RK OK      RPS      1100
9-B      - -      esent

```

This is an example of output from the show env xps system command:

```

Switch#
=====

XPS 0101.0100.0000 :
=====
XPS          Cfg  Cfg      RPS Switch  Current  Data Port  XPS Port Name
-----
Mode Role    Pri Conn  Role-State  Switch #
-----
1      -          On  Auto-SP  1  Yes      SP-PS      -
2      -          On  Auto-SP  2  Yes      SP-PS      -
3      -          On  Auto-SP  3  No       -          -
4      none       On  Auto-SP  5  No       -          -
5      -          Off  Auto-SP  6  No       -          -
6      -          On  Auto-SP  7  No       -          -
7      -          On  Auto-SP  8  No       -          -
8      -          On  Auto-SP  9  No       -          -
9      test       On  Auto-SP  4  Yes      RPS-NB

```

This is an example of output from the show env xps thermal command:

```

Switch#
=====

XPS 0101.0100.0000 :
=====
Fan  Status
----
1      OK
2      OK
3      NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK

```

This is an example of output from the show env xps upgrade command when no upgrade is occurring:

```

Switch# show env xps upgrade
No XPS is connected and upgrading.

```

These are examples of output from the show env xps upgrade command when an upgrade is in process:

```

Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
--
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
--
1 Receiving 1%
Switch# show env xps upgrade

```

```

XPS Upgrade Xfer
SW Status Prog
-- -----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- -----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.

```

This is an example of output from the show env xps version command:

```

Switch# show env xps version
=====
XPS 0022.bdd7.9b14:
=====
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18

```

Table 56: Related Commands

Command	Description
power xps(global configuration command)	Configures XPS and XPS port names.
power xps(privileged EXEC command)	Configures the XPS ports and system.

show flow monitor

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

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

Syntax Description	broker	(Optional) Displays information about the state of the broker for the flow monitor
	detail	(Optional) Displays detailed information about the flow monitor broker.
	picture	(Optional) Displays a picture of the broker state.
	name	(Optional) Specifies the name of a flow monitor.
	<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.
	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:

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

Flow Monitor FLOW-MONITOR-1:
  Description:          Used for basic traffic analysis
```

```

Flow Record:      flow-record-1
Flow Exporter:   flow-exporter-1
                  flow-exporter-2

Cache:
  Type:           normal
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
  Update Timeout:  1800 secs

```

This table describes the significant fields shown in the display.

Table 57: 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 possible values are: <ul style="list-style-type: none"> • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
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.
Update Timeout	Current value for the update timeout in seconds.

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

```

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

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

DATALINK MAC SOURCE ADDRESS INPUT:        0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:    6400.F125.59E6
IPV6 SOURCE ADDRESS:                      2001:DB8::1
IPV6 DESTINATION ADDRESS:                 2001:DB8:1::1
TRNS SOURCE PORT:                         1111
TRNS DESTINATION PORT:                   2222
IP VERSION:                               6
IP PROTOCOL:                              6
IP TOS:                                   0x05
IP TTL:                                   11
tcp flags:                                0x20
counter bytes long:                       132059538
counter packets long:                     1158417

```

This table describes the significant fields shown in the display.

Table 58: 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.

Field	Description
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

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

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

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

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

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

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

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

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

```
counter bytes long:          132059538
counter packets long:       1158417
```

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

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

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

show license right-to-use

To display detailed information for apcount adder licenses installed on the device, use the **show license right-to-use** command in EXEC modes.

show license right-to-use {**default** | **detail** | **eula** | **mismatch** | **slot** | **summary** | **usage**}

Syntax Description	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:

```
Device# show license right-to-use usage
```

Slot#	License Name	Type	usage-duration (y:m:d)	In-Use	EULA
1	ipservices	permanent	0 :0 :1	yes	yes
1	ipbase	permanent	0 :0 :0	no	no
1	ipbase	evaluation	0 :0 :0	no	no
1	lanbase	permanent	0 :0 :7	no	yes
1	apcount	evaluation	0 :0 :0	no	no
1	apcount	base	0 :0 :0	no	no
1	apcount	adder	0 :0 :0	no	yes
1	apcount	adder	0 :0 :0	no	yes
1	apcount	adder	0 :0 :0	no	yes
1	apcount	adder	0 :0 :0	no	yes

Device#

The following is sample output from the **show license right-to-use detail** command and displays the detailed information of licenses:

```
Device# show license right-to-use detail

Index 1: License Name: apcount
         Period left: 16
         License Type: evaluation
         License State: Not Activated
         License Count: 1000
         License Location: Slot 1
Index 2: License Name: apcount
         Period left: Lifetime
         License Type: adder
         License State: Active, In use
         License Count: 125
         License Location: Slot 1
```

The following is sample output from the **show license right-to-use summary** command when the evaluation license is active:

```
Device# show license right-to-use summary
  License Name      Type      Count      Period left
-----
  apcount           evaluation  1000       50
-----

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900
```

The following is sample output from the **show license right-to-use summary** command when the adder licenses are active:

```
Device# show license right-to-use summary
  License Name      Type      Count      Period left
-----
  apcount           adder      125        Lifetime
-----

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25
```

show location

To display location information, use the **show location** command in privileged EXEC mode.

```
show location {detail mac-addr | plm | statistics | summary rfid | rfid {client | config | detail MAC-addr | summary}}
```

Syntax Description		
detail <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:

```
Device# show location plm
Location Path Loss Configuration

Calbration client      : Disabled, Radio: Multiband
Normal clients         : Disabled
Burst interval         : 60
```


show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes User EXEC
Privileged EXEC

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

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show platform integrity

To display checksum record for the boot stages , use the **show platform integrity** command in privileged EXEC mode.

show platform integrity [**sign** [**nonce** <nonce>]]

Syntax Description	sign	(Optional) Show signature
	nonce	(Optional) Enter a nonce value
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2 This command was introduced.	

Examples

This example shows how to view the checksum record for boot stages :

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFF46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform sudi certificate

To display checksum record for the specific SUDI, use the **show platform sudi certificate** command in privileged EXEC mode.

show platform sudi certificate [**sign** [**nonce** <nonce>]]

Syntax Description	sign	(Optional) Show signature
	nonce	(Optional) Enter a nonce value
Command Modes	Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.3.2	This command was introduced.

Examples

This example shows how to view the checksum record for a specific SUDI :

```
Device# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDwNDGwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAlMRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDwNDGwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficia0ZmKUEIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOamaHBKeN8hF570YQXJ
FcjPftolYYmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFU14F1pyXOWWqCZe+36ufijXWLBvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTy5j/e/rmXrbU6YTYK/CdfHbBcl1HP7R2RQgYcUTOG/rksc35LTLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQa18dwy3U8pORFbi71R803UXHOjgXkhLtv5MOhmBvrbW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFpliqRe61JT37mjpXYgyc81WhJdtSd9i7rp77rMKSsH0T81asz
Bvt9YaretIjpsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe00caEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
kxpUnwVwvEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAYsGAWIBAgIKYQ1ufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDwNDGw
HhcNMTUwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEw1DaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJENBMTIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAOm5l3THixA9tN/hS5qR/6UZRpdd+9aE2JbFknjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHUMQMqmgmg+
xghHiooWS80BocdiynEbeP5rZ7qRuewKmpl1TiI3WdBNjZjnpfjg66F+P4SadkGb
BXdgj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1xtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWbf2nsVqjBDBgNVHR8EPDA6MDiGnQa0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW51cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
```

show platform sudi certificate

```

BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyaxR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZlIhvcNAQEFBQAdggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIFI9b9+GbMSJbi
ZHc/CcC10lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Ik1t8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOwryAK4dVo8hCkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LluFM2PlAs8YyjoNpK/urSRI14WdIlplR1nH7KND15618yfVp
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBGNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWjBTtjPjG
RE8xOTMyWDAAQwZEOmAwGA1UEChMFQ2l2Y28xGDAwBgNVBAsTD0FDVCOyIEExpdGUg
U1VESTeZMbcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASlWdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eU14HcSwjL4HO75qTj19C2BHG3ufce9ikkN
xwGXi8qg8vKxuB9tRYRaJC5bP1Wmoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCOzVICbnfbzvtB30I75tCarFNmpd0K6AfrIa41U988QGqaCj7R1JrYNaj
nc73UXXM/hC0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmah/KLC
K97ywyRbdJ1xBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGApm2+s8E9hsHPBPMCdIsCAwEAAANvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEAAQkVAgoG
NRMzQ2hpcE1EPVVZSk5ORmRRR1FvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbvCRjVIR5MQcWXUT086v6Ej
HahDHTs3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUoNL4szPhmmDcULfiCGBCA
/R3EFuoVMIzNT0gezitysCf728KGw1oGuosgVjNGOoahUELu4+F/My7bIJNBH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTtk09vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfyfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----

```

show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

show sdm prefer [**advanced**]

Syntax Description	advanced (Optional) Displays information on the advanced template.
---------------------------	---

Command Default	No default behavior or values.
------------------------	--------------------------------

Command Modes	Privileged EXEC
----------------------	-----------------

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

Usage Guidelines If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

Example

The following is sample output from the **show sdm prefer** command:

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:                               4094
Unicast MAC addresses:                         32768
Overflow Unicast MAC addresses:                512
IGMP and Multicast groups:                    8192
Overflow IGMP and Multicast groups:           512
Directly connected routes:                   32768
Indirect routes:                              7680
Security Access Control Entries:              3072
QoS Access Control Entries:                   3072
Policy Based Routing ACEs:                    1024
Netflow ACEs:                                 1024
Input Microflow policer ACEs:                 256
Output Microflow policer ACEs:                256
Flow SPAN ACEs:                              256
Tunnels:                                      256
```

```
Control Plane Entries:          512
Input Netflow flows:           8192
Output Netflow flows:          16384
SGT/DGT entries:                4096
SGT/DGT Overflow entries:      512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
```

```
Device#
```

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 59: Default Values for the Temperature Thresholds

Device	Difference between Yellow and Red	Red ¹¹
Catalyst 3850	14°C	60°C

¹¹ You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.



Note

The internal temperature sensor in the device measures the internal system temperature and might vary ± 5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Device(config)# system env temperature threshold yellow 15
Device(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:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has an link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

```
traceroute mac [interface interface-id] source-mac-address [interface interface-id]
destination-mac-address [vlan vlan-id] [detail]
```

Syntax Description

interface <i>interface-id</i>	(Optional) Specifies an interface on the source or destination device.
<i>source-mac-address</i>	The MAC address of the source device in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination device 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 device to the destination device. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devices in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
    Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devices:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) :   Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) :   Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) :   Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
```

```
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# tracertool mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# tracertool mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# tracertool mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# tracertool mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip {*source-ip-address source-hostname*} {*destination-ip-address destination-hostname*} [**detail**]

Syntax Description		
<i>source-ip-address</i>	The IP address of the source device as a 32-bit quantity in dotted-decimal format.	
<i>source-hostname</i>	The IP hostname of the source device.	
<i>destination-ip-address</i>	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.	
<i>destination-hostname</i>	The IP hostname of the destination device.	
detail	(Optional) Specifies that detailed information appears.	

Command Default No default behavior or values.

Command Modes Privileged EXEC

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

Usage Guidelines For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# 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:

```
Device# 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:

```
Device# tracroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

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>
-----------------	--

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset *variable...*

Syntax Description

variable

Use one of these keywords for *variable*:

MANUAL_BOOT—Specifies whether the device automatically or manually boots.

BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.

ENABLE_BREAK—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized.

HELPER—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

PS1—Specifies the string that is used as the command-line prompt in boot loader mode.

CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.

BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Usage Guidelines

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The **MANUAL_BOOT** environment variable can also be reset by using the **no boot manual** global configuration command.

The **BOOT** environment variable can also be reset by using the **no boot system** global configuration command.

The **ENABLE_BREAK** environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values.

Command Modes Boot loader

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

Examples

This example shows how to display the boot loader version on a device:

```
Device: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.3, RELEASE SOFTWARE (P)
Compiled Sun Jun 16 18:31:15 PDT 2013 by rel
```



Tracing

- [Information About Tracing, on page 988](#)
- [set platform software trace, on page 990](#)
- [show platform software trace filter-binary, on page 994](#)
- [show platform software trace message, on page 995](#)
- [show platform software trace level, on page 998](#)
- [request platform software trace archive, on page 1001](#)
- [request platform software trace rotate all, on page 1002](#)
- [request platform software trace filter-binary, on page 1003](#)

Information About Tracing

Tracing Overview

The tracing functionality logs internal events. Trace files are automatically created and saved to the `tracelogs` subdirectory under `crashinfo`.

The contents of trace files are useful for the following purposes:

- **Troubleshooting**—If a switch has an issue, the trace file output may provide information that can be used for locating and solving the issue.
- **Debugging**—The trace file outputs helps users get a more detailed view of system actions and operations.

To view the most recent trace information for a specific module, use the **show platform software trace message** command.

To modify the trace level to increase or decrease the amount of trace message output, you can set a new trace level using the **set platform software trace** command. Trace levels can be set for each process using the **all-modules** keyword in the **set platform software trace** command, or per module within a process.

Location of Tracelogs

Each process uses `btrace` infrastructure to log its trace messages. When a process is active, the corresponding in-memory tracelog is found in the directory `/tmp/<FRU>/trace/`, where `<FRU>` refers to the location where the process is running (`rp`, `fp`, or `cc`).

When a tracelog file has reached the maximum file size limit allowed for the process, or if the process ends, it gets rotated into the following directory:

- `/crashinfo/tracelogs`, if the `crashinfo`: partition is available on the switch
- `/harddisk/tracelogs`, if the `crashinfo`: partition is not available on the switch

The tracelog files are compressed before being stored in the directory.

Tracelog Naming Convention

All the tracelogs that are created using `btrace` have the following naming convention:

```
<process_name>_<FRU><SLOT>-<BAY>.<pid>_<counter>.<creation_timestamp>.bin
```

Here, `counter` is a free-running 64-bit counter that gets incremented for each new file created for the process. For example, `wcm_R0-0.1362_0.20151006171744.bin`. When compressed, the files will have the `gz` extension appended to their names

Tracelog size limits and rotation policy

The maximum size limit for a tracelog file is 1MB for each process, and the maximum number of tracelog files that are maintained for a process is 25.

Rotation and Throttling Policy

Initially, all the tracelog files are moved from the initial `/tmp/<FRU>/trace` directory to the `/tmp/<FRU>/trace/stage` staging directory. The `btrace_rotate` script then moves these tracelogs from the staging directory to the `/crashinfo/tracelogs` directory. When the number of files stored in the `/crashinfo/tracelogs` directory per process reaches the maximum limit, the oldest files for the process are deleted, while the newer files are maintained. This is repeated at every 60 minutes under worst-case situations.

There are two other sets of files that are purged from the `/crashinfo/tracelogs` directory:

- Files that do not have the standard naming convention (other than a few exceptions such as `fed_python.log`)
- Files older than two weeks

The throttling policy has been introduced so that a process with errors does not affect the functioning of the switch. Whenever a process starts logging at a very high rate, for example, if there are more than 16 files in a 4-second interval for the process in the staging directory, the process is throttled. The files do not rotate for the process from `/tmp/<FRU>/trace` into `/tmp/<FRU>/trace/stage`, however the files are deleted when they reach the maximum size. Throttling is re-enabled, when the count goes below 8.

Tracing Levels

Tracing levels determine how much information should be stored about a module in the trace buffer or file.

The following table shows all of the tracing levels that are available, and provides descriptions of the message that are displayed with each tracing level.

Table 60: Tracing Levels and Descriptions

Tracing Level	Description
Emergency	The message is regarding an issue that makes the system unusable.
Error	The message is regarding a system error.
Warning	The message is regarding a system warning.
Notice	The message is regarding a significant issue, but the switch is still working normally.
Informational	The message is useful for informational purposes only.
Debug	The message provides debug-level output.
Verbose	All possible trace messages are sent.
Noise	All possible trace messages for the module are logged. The noise level is always equal to the highest possible tracing level. Even if a future enhancement to tracing introduces a higher tracing level, the noise level will become equal to the level of that new enhancement.

set platform software trace

To set the trace level for a specific module within a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

set platform software trace *process slot module trace-level*

Syntax Description

process

Process whose tracing level is being set. Options include:

- **chassis-manager**—The Chassis Manager process.
 - **cli-agent**—The CLI Agent process.
 - **dbm**—The Database Manager process.
 - **emd**—The Environmental Monitoring process.
 - **fed**—The Forwarding Engine Driver process.
 - **forwarding-manager**—The Forwarding Manager process.
 - **host-manager**—The Host Manager process.
 - **iomd**—The Input/Output Module daemon (IOMd) process.
 - **ios**—The IOS process.
 - **license-manager**—The License Manager process.
 - **logger**—The Logging Manager process.
 - **platform-mgr**—The Platform Manager process.
 - **pluggable-services**—The Pluggable Services process.
 - **replication-mgr**—The Replication Manager process.
 - **shell-manager**—The Shell Manager process.
 - **smd**—The Session Manager process.
 - **table-manager**—The Table Manager Server.
 - **wireshark**—The Embedded Packet Capture (EPC) Wireshark process.
-

<i>slot</i>	<p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none">• <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.• <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.• F0—The Embedded-Service-Processor in slot 0.• FP active—The active Embedded-Service-Processor.• R0—The route processor in slot 0.• RP active—The active route processor.• switch <number> —The switch with its number specified.• switch active—The active switch.• switch standby—The standby switch.
<i>module</i>	Module within the process for which the tracing level is set.

trace-level

Trace level. Options include:

- **debug**—Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module.
- **emergency**—Emergency level tracing. An emergency-level trace message is a message indicating that the system is unusable.
- **error**—Error level tracing. An error-level tracing message is a message indicating a system error.
- **info**—Information level tracing. An information-level tracing message is a non-urgent message providing information about the system.
- **noise**—Noise level tracing. The noise level is always equal to the highest tracing level possible and always generates every possible tracing message.
The noise level is always equal to the highest-level tracing message possible for a module, even if future enhancements to this command introduce options that allow users to set higher tracing levels.
- **notice**—The message is regarding a significant issue, but the switch is still working normally.
- **verbose**—Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose.
- **warning**—Warning messages.

Command Default The default tracing level for all modules is **notice**.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines The *module* options vary by process and by *hardware-module*. Use the ? option when entering this command to see which *module* options are available with each keyword sequence.

Use the **show platform software trace message** command to view trace messages.

Trace files are stored in the tracelogs directory in the harddisk: file system. These files can be deleted without doing any harm to your switch operation.

Trace file output is used for debugging. The trace level is a setting that determines how much information should be stored in trace files about a module.

Examples

This example shows how to set the trace level for all the modules in dbm process:

```
Device# set platform software trace dbm R0 all-modules debug
```

show platform software trace filter-binary

To display the most recent trace information for a specific module, use the **show platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

show platform software trace filter-binary*modules* [**context** *mac-address*]

Syntax Description	context <i>mac-address</i>	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.
Command Modes	User EXEC (>) Privileged EXEC (#)	
Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.
Usage Guidelines	This command collates and sorts all the logs present in the /tmp/. . ./ across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the /crashinfo/tracelogs directory.	

show platform software trace message

To display the trace messages for a process, use the **set platform software trace** command in privileged EXEC or user EXEC mode.

show platform software trace message *process slot*

Syntax Description

process

Tracing level that is being set. Options include:

- **chassis-manager**—The Chassis Manager process.
 - **cli-agent**—The CLI Agent process.
 - **cmm**—The CMM process.
 - **dbm**—The Database Manager process.
 - **emd**—The Environmental Monitoring process.
 - **fed**—The Forwarding Engine Driver process.
 - **forwarding-manager**—The Forwarding Manager process.
 - **geo**—The Geo Manager process.
 - **host-manager**—The Host Manager process.
 - **interface-manager**—The Interface Manager process.
 - **iomd**—The Input/Output Module daemon (IOMd) process.
 - **ios**—The IOS process.
 - **license-manager**—The License Manager process.
 - **logger**—The Logging Manager process.
 - **platform-mgr**—The Platform Manager process.
 - **pluggable-services**—The Pluggable Services process.
 - **replication-mgr**—The Replication Manager process.
 - **shell-manager**—The Shell Manager process.
 - **sif**—The Stack Interface (SIF) Manager process.
 - **smd**—The Session Manager process.
 - **stack-mgr**—The Stack Manager process.
 - **table-manager**—The Table Manager Server.
 - **thread-test**—The Multithread Manager process.
 - **virt-manager**—The Virtualization Manager process.
-

slot

Hardware slot where the process for which the trace level is set, is running. Options include:

- *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
- *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
- **F0**—The Embedded Service Processor slot 0.
- **FP active**—The active Embedded Service Processor.
- **R0**—The route processor in slot 0.
- **RP active**—The active route processor.
- **switch <number>** —The switch, with its number specified.
- **switch active**—The active switch.
- **switch standby**—The standby switch.
 - *number*—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.
 - *SIP-slot / SPA-bay*—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.
 - **F0**—The Embedded Service Processor in slot 0.
 - **FP active**—The active Embedded Service Processor.
 - **R0**—The route processor in slot 0.
 - **RP active**—The active route processor.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Examples

This example shows how to display the trace messages for the Stack Manager and the Forwarding Engine Driver processes:

```
Device# show platform software trace message stack-mgr switch active R0
10/30 09:42:48.767 [btrace] [8974]: (note): Successfully registered module [97] [uiutil]
10/30 09:42:48.762 [btrace] [8974]: (note): Successfully registered module [98]
[tdl_cdlcore_message]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state
10/29 13:28:19.023 [stack_mgr] [8974]: (note): no switch eligible for standby election
presently
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Posting event
stack_fsm_event_wait_standby_elect_timer_expired, curstate stack_fsm_state_active_ready
10/29 13:28:19.022 [stack_mgr] [8974]: (note): Timer HDL - STACK_WAIT_STANDBY_ELECT_TIMER
expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
[tdl_ui_message]
10/29 13:26:46.582 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:36.582 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect
10/29 13:26:36.582 [evutil] [8974]: (ERR): Asynchronous connect failed for [uipeer uplink
to slot 1] (fd == -1)
10/29 13:26:36.581 [bipc] [8974]: (note): Pending connection to server 10.129.1.0
10/29 13:26:26.581 [evutil] [8974]: (ERR): Connection attempt for sman-ui-serv (uipeer
uplink to slot 1) failed, invoking disconnect

Device# show platform software trace message fed switch active
11/02 10:55:01.832 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[86] [uiutil]
11/02 10:55:01.848 [btrace]: [11310]: UUID: 0, ra: 0 (note): Single message size is greater
than 1024
11/02 10:55:01.822 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[87] [tdl_cdlcore_message]
11/01 09:54:41.474 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[88] [tdl_ngwc_gold_message]
11/01 09:54:11.228 [btrace]: [12312]: UUID: 0, ra: 0 (note): Successfully registered module
[89] [tdl_doppler_iosd_matm_type]
11/01 09:53:37.454 [btrace]: [11310]: UUID: 0, ra: 0 (note): Successfully registered module
[90] [tdl_ui_message]
11/01 09:53:37.382 [bipc]: [11310]: UUID: 0, ra: 0 (note): Pending connection to server
10.129.1.0
11/01 09:53:34.227 [xcvr]: [18846]: UUID: 0, ra: 0 (ERR): FRU hardware authentication Fail,
result = 1.
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR): SMART COOKIE: SCC I2C receive
failed: rc=10
11/01 09:53:33.775 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
SMART COOKIE receive failed, try again
11/01 09:53:33.585 [ng3k_scc]: [18846]: UUID: 0, ra: 0 (ERR):
```

show platform software trace level

To view the trace levels for all the modules under a specific process, use the **show platform software trace level** command in privileged EXEC or user EXEC mode.

show platform software trace level *process slot*

Syntax Description

process

Process whose tracing level is being set. Options include:

- **chassis-manager**—The Chassis Manager process.
 - **cli-agent**—The CLI Agent process.
 - **cmm**—The CMM process.
 - **dbm**—The Database Manager process.
 - **emd**—The Environmental Monitoring process.
 - **fed**—The Forwarding Engine Driver process.
 - **forwarding-manager**—The Forwarding Manager process.
 - **geo**—The Geo Manager process.
 - **host-manager**—The Host Manager process.
 - **interface-manager**—The Interface Manager process.
 - **iomd**—The Input/Output Module daemon (IOMd) process.
 - **ios**—The IOS process.
 - **license-manager**—The License Manager process.
 - **logger**—The Logging Manager process.
 - **platform-mgr**—The Platform Manager process.
 - **pluggable-services**—The Pluggable Services process.
 - **replication-mgr**—The Replication Manager process.
 - **shell-manager**—The Shell Manager process.
 - **sif**—The Stack Interface (SIF) Manager process.
 - **smd**—The Session Manager process.
 - **stack-mgr**—The Stack Manager process.
 - **table-manager**—The Table Manager Server.
 - **thread-test**—The Multithread Manager process.
 - **virt-manager**—The Virtualization Manager process.
-

<i>slot</i>	<p>Hardware slot where the process for which the trace level is set, is running. Options include:</p> <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • F1—The Embedded Service Processor in slot 1. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor. • switch <number> —The switch, with its number specified. • switch active—The active switch. • switch standby—The standby switch. <ul style="list-style-type: none"> • <i>number</i>—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2. • <i>SIP-slot / SPA-bay</i>—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2. • F0—The Embedded Service Processor in slot 0. • FP active—The active Embedded Service Processor. • R0—The route processor in slot 0. • RP active—The active route processor.
-------------	---

Command Modes	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Examples This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
```

show platform software trace level

Module Name	Trace Level
-----	-----
binos	Notice
binos/brand	Notice
bipc	Notice
btrace	Notice
bump_ptr_alloc	Notice
cdllib	Notice
chasfs	Notice
dbal	Informational
dbm	Debug
evlib	Notice
evutil	Notice
file_alloc	Notice
green-be	Notice
ios-avl	Notice
klib	Debug
services	Notice
sw_wdog	Notice
syshw	Notice
tcl_cdlcore_message	Notice
tcl_dbal_root_message	Notice
tcl_dbal_root_type	Notice

request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the switches and to save this in the specified location, use the **request platform software trace archive** command in privileged EXEC or user EXEC mode.

request platform software trace archive [**last** *number-of-days* [**days** [**target** *location*]] | **target** *location*]

Syntax Description		
last <i>number-of-days</i>		Specifies the number of days for which the trace files have to be archived.
target <i>location</i>		Specifies the location and name of the archive file.

Command Modes	
	User EXEC (>)
	Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines This archive file can be copied from the system, using the tftp or scp commands.

Examples This example shows how to archive all the trace logs of the processes running on the switch since the last 5 days:

```
Device# request platform software trace archive last 5 days target flash:test_archive
```

request platform software trace rotate all

To rotate all the current in-memory trace logs into the crashinfo partition and start a new in-memory trace log for each process, use the **request platform software trace rotate all** command in privileged EXEC or user EXEC mode.

request platform software trace rotate all

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

The trace log files are for read-only purpose. Do not edit the contents of the file. If there is a requirement to delete the contents of the file to view certain set of logs, use this command to start a new trace log file.

Examples

This example shows how to rotate all the in-memory trace logs of the processes running on the switch since the last one day:

```
Device# request platform software trace slot switch active R0 archive last 1 days target
flash:test
```

request platform software trace filter-binary

To collate and sort all the archived logs present in the `tracelogs` subdirectory, use the **request platform software trace filter-binary** command in privileged EXEC or user EXEC mode.

```
request platform software trace filter-binary modules [context mac-address]
```

Syntax Description	context <i>mac-address</i>	Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged.
---------------------------	-----------------------------------	--

Command Modes	User EXEC (>) Privileged EXEC (#)
----------------------	--------------------------------------

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines	This command collates and sorts all the archived logs present in the <code>tracelogs</code> subdirectory, across all the processes relevant to the module. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> directory.
-------------------------	--



PART **XV**

VLAN

- [VLAN, on page 1007](#)



VLAN

- [clear l2protocol-tunnel counters](#), on page 1008
- [clear vmpls statistics](#), on page 1009
- [clear vtp counters](#), on page 1010
- [debug platform vlan](#), on page 1011
- [debug sw-vlan](#), on page 1012
- [debug sw-vlan ifs](#), on page 1014
- [debug sw-vlan notification](#), on page 1015
- [debug sw-vlan vtp](#), on page 1016
- [interface vlan](#), on page 1018
- [l2protocol-tunnel](#), on page 1019
- [l2protocol-tunnel cos](#), on page 1022
- [private-vlan](#), on page 1023
- [private-vlan mapping](#), on page 1025
- [show dot1q-tunnel](#), on page 1027
- [show interfaces private-vlan mapping](#), on page 1028
- [show l2protocol-tunnel](#), on page 1029
- [show platform vlan](#), on page 1031
- [show vlan](#), on page 1032
- [show vmpls](#), on page 1036
- [show vtp](#), on page 1038
- [switchport mode private-vlan](#), on page 1044
- [switchport priority extend](#), on page 1046
- [switchport trunk](#), on page 1047
- [vlan](#), on page 1050
- [vlan dot1q tag native](#), on page 1056
- [vmpls reconfirm \(global configuration\)](#), on page 1057
- [vmpls reconfirm \(privileged EXEC\)](#), on page 1058
- [vmpls retry](#), on page 1059
- [vmpls server](#), on page 1060
- [vtp \(global configuration\)](#), on page 1061
- [vtp \(interface configuration\)](#), on page 1066
- [vtp primary](#), on page 1067

clear l2protocol-tunnel counters

To clear the protocol counters in protocol tunnel ports, use the **clear l2protocol-tunnel counters** command in privileged EXEC mode.

```
clear l2protocol-tunnel counters [interface-id]
```

Syntax Description	<i>interface-id</i>	(Optional) The interface (physical interface or port channel) for which protocol counters are to be cleared.
---------------------------	---------------------	--

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 to clear protocol tunnel counters on the switch or on the specified interface.
-------------------------	---

This example shows how to clear Layer 2 protocol tunnel counters on an interface:

```
Device# clear l2protocol-tunnel counters gigabitethernet1/0/3
```


clear vmps statistics

To clear the VLAN Membership Policy Server (VMPS) statistics maintained by the VLAN Query Protocol (VQP) client, use the **clear vmps statistics** command in privileged EXEC mode.

clear vmps statistics

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 VLAN Membership Policy Server (VMPS) statistics:

```
Device# clear vmps statistics
```

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

clear vtp counters

To clear the VLAN Trunking Protocol (VTP) and pruning counters, use the **clear vtp counters** command in privileged EXEC mode.

clear vtp counters

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC

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

This example shows how to clear the VTP counters:

```
Device# clear vtp counters
```

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

debug platform vlan

To enable debugging of the VLAN manager software, use the **debug platform vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

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

Syntax Description	
error	(Optional) Displays VLAN error debug messages.
event	(Optional) Displays VLAN platform event debug messages.
switch <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 **undebg platform vlan** command is the same as the **no debug platform vlan** command.

This example shows how to display VLAN error debug messages:

```
Device# debug platform vlan error
```

debug sw-vlan

To enable debugging of VLAN manager activities, use the **debug sw-vlan** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan {bootup | cli} | events | ifs | management | mapping | notification | packets | redundancy | registries | vtp}

Syntax Description

badpmcookies	Displays debug messages for VLAN manager incidents of bad port manager cookies.
cfg-vlan	Displays VLAN configuration debug messages.
bootup	Displays messages when the switch is booting up.
cli	Displays messages when the command-line interface (CLI) is in VLAN configuration mode.
events	Displays debug messages for VLAN manager events.
ifs	Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 1014 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 1015 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 1016 for more information.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch *stack-member-number*** privileged EXEC command.

This example shows how to display debug messages for VLAN manager events:

```
Device# debug sw-vlan events
```

debug sw-vlan ifs

To enable debugging of the VLAN manager IOS file system (IFS) error tests, use the **debug sw-vlan ifs** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
no debug sw-vlan ifs {open {read | write} | read {1 | 2 | 3 | 4} | write}
```

Syntax Description		
open read	Displays VLAN manager IFS file-read operation debug messages.	
open write	Displays VLAN manager IFS file-write operation debug messages.	
read	Displays file-read operation debug messages for the specified error test (1 , 2 , 3 , or 4).	
write	Displays file-write operation debug messages.	

Command Default Debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines The **undebg sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch stack-member-number** privileged EXEC command.

This example shows how to display file-write operation debug messages:

```
Device# debug sw-vlan ifs write
```

debug sw-vlan notification

To enable debugging of VLAN manager notifications, use the **debug sw-vlan notification** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

no debug sw-vlan notification {accfwdchange | allowedvlanfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

Syntax Description		
accfwdchange	Displays debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes.	
allowedvlanfgchange	Displays debug messages for VLAN manager notification of changes to the allowed VLAN configuration.	
fwdchange	Displays debug messages for VLAN manager notification of spanning-tree forwarding changes.	
linkchange	Displays debug messages for VLAN manager notification of interface link-state changes.	
modechange	Displays debug messages for VLAN manager notification of interface mode changes.	
pruningcfgchange	Displays debug messages for VLAN manager notification of changes to the pruning configuration.	
statechange	Displays debug messages for VLAN manager notification of interface state changes.	

Command Default Debugging is disabled.

Command Modes Privileged EXEC

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

Usage Guidelines The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command. When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch stack-member-number** privileged EXEC command.

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Device# debug sw-vlan notification
```

debug sw-vlan vtp

To enable debugging of the VLAN Trunking Protocol (VTP) code, use the **debug sw-vlan vtp** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

```
debug sw-vlan vtp {events | packets | pruning [{packets | xmit}] | redundancy | xmit}
no debug sw-vlan vtp {events | packets | pruning | redundancy | xmit}
```

Syntax Description

events	Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.
packets	Displays debug messages for the contents of all incoming VTP packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer, except for pruning packets.
pruning	Displays debug messages generated by the pruning segment of the VTP code.
packets	(Optional) Displays debug messages for the contents of all incoming VTP pruning packets that have been passed into the VTP code from the Cisco IOS VTP platform-dependent layer.
xmit	(Optional) Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send.
redundancy	Displays debug messages for VTP redundancy.
xmit	Displays debug messages for the contents of all outgoing VTP packets that the VTP code requests the Cisco IOS VTP platform-dependent layer to send, except for pruning packets.

Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The **undebug sw-vlan vtp** command is the same as the **no debug sw-vlan vtp** command.

If no additional parameters are entered after the **pruning** keyword, VTP pruning debugging messages appear. They are generated by the VTP_PRUNING_LOG_NOTICE, VTP_PRUNING_LOG_INFO, VTP_PRUNING_LOG_DEBUG, VTP_PRUNING_LOG_ALERT, and VTP_PRUNING_LOG_WARNING macros in the VTP pruning code.

When you enable debugging on a switch stack, it is enabled only on the active switch. To debug a specific stack member, you can start a CLI session from the active switch by using the **session switch stack-member-number** privileged EXEC command.

This example shows how to display debug messages for VTP redundancy:

```
Device# debug sw-vlan vtp redundancy
```

interface vlan

To create or access a dynamic switch virtual interface (SVI) and to enter interface configuration mode, use the **interface vlan** command in global configuration mode. To delete an SVI, use the **no** form of this command.

interface vlan *vlan-id*
no interface vlan *vlan-id*

Syntax Description

vlan-id VLAN number. The range is 1 to 4094.

Command Default

The default VLAN interface is VLAN 1.

Command Modes

Global configuration

Command History

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

Usage Guidelines

SVIs are created the first time you enter the **interface vlan** *vlan-id* command for a particular VLAN. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.



Note

When you create an SVI, it does not become active until it is associated with a physical port.

If you delete an SVI using the **no interface vlan** *vlan-id* command, it is no longer visible in the output from the **show interfaces** privileged EXEC command.



Note

You cannot delete the VLAN 1 interface.

You can reinstate a deleted SVI by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but the previous configuration is gone.

The interrelationship between the number of SVIs configured on a switch or a switch stack and the number of other features being configured might have an impact on CPU utilization due to hardware limitations. You can use the **sdm prefer** global configuration command to reallocate system hardware resources based on templates and feature tables.

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

This example shows how to create a new SVI with VLAN ID 23 and enter interface configuration mode:

```
Device(config)# interface vlan 23
Device(config-if)#
```

l2protocol-tunnel

To enable tunneling of Layer 2 protocols on an access port, IEEE 802.1Q tunnel port, or a port channel, use the **l2protocol-tunnel** command in interface configuration mode on the switch stack or on a standalone switch. Use the **no** form of this command to disable tunneling on the interface.

```
l2protocol-tunnel [{drop-threshold | shutdown-threshold}] [value] [{cdp | stp | vtp}] [lldp]
[point-to-point | [pagp | lacp | udld]]]
no l2protocol-tunnel [{drop-threshold | shutdown-threshold}] [value] [{cdp | stp | vtp}] [lldp]
[point-to-point | [pagp | lacp | udld]]]
```

Syntax Description	
drop-threshold	(Optional) Sets a drop threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface drops packets.
shutdown-threshold	(Optional) Sets a shutdown threshold for the maximum rate of Layer 2 protocol packets per second to be received before an interface is shut down.
<i>value</i>	A threshold in packets per second to be received for encapsulation before the interface shuts down, or the threshold before the interface drops packets. The range is 1 to 4096. The default is no threshold.
cdp	(Optional) Enables tunneling of CDP, specifies a shutdown threshold for CDP, or specifies a drop threshold for CDP.
stp	(Optional) Enables tunneling of STP, specifies a shutdown threshold for STP, or specifies a drop threshold for STP.
vtp	(Optional) Enables tunneling or VTP, specifies a shutdown threshold for VTP, or specifies a drop threshold for VTP.
lldp	(Optional) Enables tunneling of LLDP packets.
point-to-point	(Optional) Enables point-to-point tunneling of PAGP, LACP, and UDLD packets.
pagp	(Optional) Enables point-to-point tunneling of PAGP, specifies a shutdown threshold for PAGP, or specifies a drop threshold for PAGP.
lacp	(Optional) Enables point-to-point tunneling of LACP, specifies a shutdown threshold for LACP, or specifies a drop threshold for LACP.
udld	(Optional) Enables point-to-point tunneling of UDLD, specifies a shutdown threshold for UDLD, or specifies a drop threshold for UDLD.

Command Default

The default is that no Layer 2 protocol packets are tunneled.

The default is no shutdown threshold for the number of Layer 2 protocol packets.

The default is no drop threshold for the number of Layer 2 protocol packets.

Command Modes

Interface configuration

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

Usage Guidelines

You can enable tunneling for Cisco Discovery Protocol (CDP), Spanning Tree Protocol (STP), or VLAN Trunking Protocol (VTP) packets. You can also enable point-to-point tunneling for Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or UniDirectional Link Detection (UDLD) packets.

You must enter this command, with or without protocol types, to tunnel Layer 2 packets.

If you enter this command for a port channel, all ports in the channel must have the same configuration.

Layer 2 protocol tunneling across a service-provider network ensures that Layer 2 information is propagated across the network to all customer locations. When protocol tunneling is enabled, protocol packets are encapsulated with a well-known Cisco multicast address for transmission across the network. When the packets reach their destination, the well-known MAC address is replaced by the Layer 2 protocol MAC address.

You can enable Layer 2 protocol tunneling for CDP, STP, and VTP individually or for all three protocols.

In a service-provider network, you can use Layer 2 protocol tunneling to enhance the creation of EtherChannels by emulating a point-to-point network topology. When protocol tunneling is enabled on the service-provider switch for PAgP or LACP, remote customer switches receive the protocol data units (PDUs) and can negotiate automatic creation of EtherChannels.

To enable tunneling of PAgP, LACP, and UDLD packets, you must have a point-to-point network topology. To decrease the link-down detection time, you should also enable UDLD on the interface when you enable tunneling of PAgP or LACP packets.

You can enable point-to-point protocol tunneling for PAgP, LACP, and UDLD individually or for all three protocols.



Caution

PAgP, LACP, and UDLD tunneling is only intended to emulate a point-to-point topology. An erroneous configuration that sends tunneled packets to many ports could lead to a network failure.

Enter the **shutdown-threshold** keyword to control the number of protocol packets per second that are received on an interface before it shuts down. When no protocol option is specified with the keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a drop threshold on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

When the shutdown threshold is reached, the interface is error-disabled. If you enable error recovery by entering the **errdisable recovery cause l2ptguard** global configuration command, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out. If the error recovery function is not enabled for **l2ptguard**, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

Enter the **drop-threshold** keyword to control the number of protocol packets per second that are received on an interface before it drops packets. When no protocol option is specified with a keyword, the threshold is applied to each of the tunneled Layer 2 protocol types. If you also set a shutdown threshold on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

When the drop threshold is reached, the interface drops Layer 2 protocol packets until the rate at which they are received is below the drop threshold.

The configuration is saved in NVRAM.

For more information about Layer 2 protocol tunneling, see the software configuration guide for this release.

Examples

This example shows how to enable protocol tunneling for CDP packets and to configure the shutdown threshold as 50 packets per second:

```
Device(config-if)# l2protocol-tunnel cdp
Device(config-if)# l2protocol-tunnel shutdown-threshold cdp 50
```

This example shows how to enable protocol tunneling for STP packets and to configure the drop threshold as 400 packets per second:

```
Device(config-if)# l2protocol-tunnel stp
Device(config-if)# l2protocol-tunnel drop-threshold stp 400
```

This example shows how to enable point-to-point protocol tunneling for PAgP and UDLD packets and to configure the PAgP drop threshold as 1000 packets per second:

```
Device(config-if)# l2protocol-tunnel point-to-point pagp
Device(config-if)# l2protocol-tunnel point-to-point udld
Device(config-if)# l2protocol-tunnel drop-threshold point-to-point pagp 1000
```

l2protocol-tunnel cos

To configure class of service (CoS) value for all tunneled Layer 2 protocol packets, use the **l2protocol-tunnel cos** global configuration command. To return to the default setting, use the **no** form of this command.

l2protocol-tunnel cos *value*
no l2protocol-tunnel cos

Syntax Description

value CoS priority value for tunneled Layer 2 protocol packets. If a CoS value is configured for data packets for the interface, the default is to use this CoS value. If no CoS value is configured for the interface, the default is 5. The range is 0 to 7, with 7 being the highest priority.

Command Default

The default is to use the CoS value configured for data on the interface. If no CoS value is configured, the default is 5 for all tunneled Layer 2 protocol packets.

Command Modes

Global configuration

Command History

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

Usage Guidelines

When enabled, the tunneled Layer 2 protocol packets use this CoS value.
 The value is saved in NVRAM.

Examples

This example shows how to configure a Layer-2 protocol-tunnel CoS value of 7:

```
Device(config)# l2protocol-tunnel cos 7
```

private-vlan

To configure private VLANs and to configure the association between private VLAN primary and secondary VLANs, use the **private-vlan** VLAN configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

```
private-vlan {association [{add | remove}] secondary-vlan-list | community | isolated | primary}
no private-vlan {association | community | isolated | primary}
```

Syntax Description		
association		Creates an association between the primary VLAN and a secondary VLAN.
add		Associates a secondary VLAN to a primary VLAN.
remove		Clears the association between a secondary VLAN and a primary VLAN.
<i>secondary-vlan-list</i>		One or more secondary VLANs to be associated with a primary VLAN in a private VLAN.
community		Designates the VLAN as a community VLAN.
isolated		Designates the VLAN as an isolated VLAN.
primary		Designates the VLAN as a primary VLAN.

Command Default The default is to have no private VLANs configured.

Command Modes VLAN configuration

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

Usage Guidelines Before configuring private VLANs, you must disable VTP (VTP mode transparent). After you configure a private VLAN, you should not change the VTP mode to client or server.

VTP does not propagate private VLAN configurations. You must manually configure private VLANs on all switches in the Layer 2 network to merge their Layer 2 databases and to prevent flooding of private VLAN traffic.

You cannot include VLAN 1 or VLANs 1002 to 1005 in the private VLAN configuration. Extended VLANs (VLAN IDs 1006 to 4094) can be configured in private VLANs.

You can associate a secondary (isolated or community) VLAN with only one primary VLAN. A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.

- A secondary VLAN cannot be configured as a primary VLAN.
- The *secondary-vlan-list* cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

- If you delete either the primary or secondary VLANs, the ports associated with the VLAN become inactive.

A community VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN.

An isolated VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or isolated ports with the same primary VLAN domain.

A primary VLAN is the VLAN that carries traffic from a gateway to customer end stations on private ports.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The **private-vlan** commands do not take effect until you exit from VLAN configuration mode.

Do not configure private VLAN ports as EtherChannels. While a port is part of the private VLAN configuration, any EtherChannel configuration for it is inactive.

Do not configure a private VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN.

Do not configure a private VLAN as a voice VLAN.

Do not configure fallback bridging on switches with private VLANs.

Although a private VLAN contains more than one VLAN, only one STP instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

For more information about private VLAN interaction with other features, see the software configuration guide for this release.

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, and VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN:

```
Device# configure terminal
Device(config)# vlan 20
Device(config-vlan)# private-vlan primary
Device(config-vlan)# exit
Device(config)# vlan 501
Device(config-vlan)# private-vlan isolated
Device(config-vlan)# exit
Device(config)# vlan 502
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 503
Device(config-vlan)# private-vlan community
Device(config-vlan)# exit
Device(config)# vlan 20
Device(config-vlan)# private-vlan association 501-503
Device(config-vlan)# end
```

You can verify your setting by entering the **show vlan private-vlan** or **show interfaces status privileged EXEC** command.

private-vlan mapping

To create a mapping between the primary and the secondary VLANs so that both VLANs share the same primary VLAN switched virtual interface (SVI), use the **private-vlan mapping** interface configuration command on a switch virtual interface (SVI). Use the **no** form of this command to remove private VLAN mappings from the SVI.

```
private-vlan mapping [{add | remove}] secondary-vlan-list
no private-vlan mapping
```

Syntax Description	add	(Optional) Maps the secondary VLAN to the primary VLAN SVI.
	remove	(Optional) Removes the mapping between the secondary VLAN and the primary VLAN SVI.
	<i>secondary-vlan-list</i>	One or more secondary VLANs to be mapped to the primary VLAN SVI.

Command Default No private VLAN SVI mapping is configured.

Command Modes Interface configuration

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

Usage Guidelines

The device must be in VTP transparent mode when you configure private VLANs.

The SVI of the primary VLAN is created at Layer 3.

Configure Layer 3 VLAN interfaces (SVIs) only for primary VLANs. You cannot configure Layer 3 VLAN interfaces for secondary VLANs. SVIs for secondary VLANs are inactive while the VLAN is configured as a secondary VLAN.

The *secondary-vlan-list* argument cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private VLAN ID or a hyphenated range of private VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

Traffic that is received on the secondary VLAN is routed by the SVI of the primary VLAN.

A secondary VLAN can be mapped to only one primary SVI. If you configure the primary VLAN as a secondary VLAN, all SVIs specified in this command are brought down.

If you configure a mapping between two VLANs that do not have a valid Layer 2 private VLAN association, the mapping configuration does not take effect.

This example shows how to map the interface of VLAN 20 to the SVI of VLAN 18:

```
Device# configure terminal
Device# interface vlan 18
Device(config-if)# private-vlan mapping 20
Device(config-vlan)# end
```

This example shows how to permit routing of secondary VLAN traffic from secondary VLANs 303 to 305 and 307 through VLAN 20 SVI:

```
Device# configure terminal
Device# interface vlan 20
Device(config-if)# private-vlan mapping 303-305, 307
Device(config-vlan)# end
```

You can verify your settings by entering the **show interfaces private-vlan mapping** privileged EXEC command.

show dot1q-tunnel

To display information about IEEE 802.1Q tunnel ports, use the **show dot1q-tunnel** in EXEC mode.

```
show dot1q-tunnel [interface interface-id]
```

Syntax Description	interface interface-id (Optional) Specifies the interface for which to display IEEE 802.1Q tunneling information. Valid interfaces include physical ports and port channels.				
Command Default	None				
Command Modes	User EXEC 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.				

Examples

The following are examples of output from the **show dot1q-tunnel** command:

```
Device# show dot1q-tunnel
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
Gi1/0/2
Gi1/0/3
Gi1/0/6
Po2
```

```
Device# show dot1q-tunnel interface gigabitethernet1/0/1
dot1q-tunnel mode LAN Port(s)
-----
Gi1/0/1
```

show interfaces private-vlan mapping

To display private VLAN mapping information for the VLAN switch virtual interfaces (SVIs), use the **show interfaces private-vlan mapping** command in user EXEC or privileged EXEC mode.

show interfaces [*interface-id*] **private-vlan mapping**

Syntax Description	<i>interface-id</i> (Optional) ID of the interface for which to display private VLAN mapping information.	
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 information about the private VLAN mapping:

```
Device#show interfaces private-vlan mapping
Interface Secondary VLAN Type
-----
vlan2      301      community
vlan3      302      community
```

show l2protocol-tunnel

To display information about Layer 2 protocol tunnel ports, use the **show l2protocol-tunnel** in EXEC mode.

show l2protocol-tunnel [**interface** *interface-id*] **summary**

Syntax Description	interface <i>interface-id</i> (Optional) Specifies the interface for which protocol tunneling information appears. Valid interfaces are physical ports and port channels; the port channel range is 1 to 48.
	summary (Optional) Displays only Layer 2 protocol summary 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 After enabling Layer 2 protocol tunneling on an access or IEEE 802.1Q tunnel port by using the **l2protocol-tunnel** interface configuration command, you can configure some or all of these parameters:

- Protocol type to be tunneled
- Shutdown threshold
- Drop threshold

If you enter the **show l2protocol-tunnel interface** command, only information about the active ports on which all the parameters are configured appears.

If you enter the **show l2protocol-tunnel summary** command, only information about the active ports on which some or all of the parameters are configured appears.

Examples

This is an example of output from the **show l2protocol-tunnel** command:

```
Switch> show l2protocol-tunnel
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0
```

Port	Protocol	Shutdown Threshold	Drop Threshold	Encapsulation Counter	Decapsulation Counter	Drop Counter
Gi3/0/3	---	----	----	----	----	----
	pagp	----	----	0	242500	----
	lacp	----	----	24268	242640	----
	udld	----	----	0	897960	----
Gi3/0/4	---	----	----	----	----	----
	---	----	----	----	----	----

```

          ---          ----          ----          ----          ----          ----
          pagp          1000          ----          24249          242700          ----
          lacp          ----          ----          24256          242660          ----
          udld          ----          ----          0          897960          ----
Gi6/0/1  cdp          ----          ----          134482          1344820          ----
          ----          ----          ----          ----          ----          ----
          ----          ----          ----          ----          ----          ----
          pagp          1000          ----          0          242500          ----
          lacp          500          ----          0          485320          ----
          udld          300          ----          44899          448980          ----
Gi6/0/2  cdp          ----          ----          134482          1344820          ----
          ----          ----          ----          ----          ----          ----
          ----          ----          ----          ----          ----          ----
          pagp          ----          1000          0          242700          ----
          lacp          ----          ----          0          485220          ----
          udld          300          ----          44899          448980          ----

```

This is an example of output from the **show l2protocol-tunnel summary** command:

```

Switch> show l2protocol-tunnel summary
COS for Encapsulated Packets: 5
Drop Threshold for Encapsulated Packets: 0

Port      Protocol      Shutdown      Drop      Status
          Protocol      Threshold      Threshold
          (cdp/stp/vtp) (cdp/stp/vtp)
          (pagp/lacp/udld) (pagp/lacp/udld)
-----
Gi3/0/2  pagp lacp udld  ----/----/----  ----/----/----  up
Gi4/0/3  pagp lacp udld  1000/ 500/----  ----/----/----  up
Gi9/0/1  pagp ---- ----  ----/----/----  1000/----/----  down
Gi9/0/2  pagp ---- ----  ----/----/----  1000/----/----  down

```

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:

```
Device# show platform vlan
```

show vlan

To display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch, use the **show vlan** command in user EXEC mode.

```
show vlan [{brief | dot1q tag native | group | id vlan-id | mtu | name vlan-name | private-vlan
[{type}]} | 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.	
private-vlan	(Optional) Displays information about configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and ports belonging to the private VLAN. This keyword is only supported if your switch is running the IP services feature set.	
type	(Optional) Displays only private VLAN ID and type.	
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.

If you try to associate a private VLAN secondary VLAN with a primary VLAN before you define the secondary VLAN, the secondary VLAN is not included in the **show vlan private-vlan** command output.

In the **show vlan private-vlan type** command output, a type displayed as normal means a VLAN that has a private VLAN association but is not part of the private VLAN. For example, if you define and associate two VLANs as primary and secondary VLANs and then delete the secondary VLAN configuration without removing the association from the primary VLAN, the VLAN that was the secondary VLAN is shown as normal in the display. In the **show vlan private-vlan** output, the primary and secondary VLAN pair is shown as nonoperational.

This is an example of output from the **show vlan** command. See the table that follows for descriptions of the fields in the display.

```
Device> show vlan
VLAN Name                Status      Ports
-----
1    default                active      Gi1/0/2, Gi1/0/3, Gi1/0/4
                                           Gi1/0/5, Gi1/0/6, Gi1/0/7
                                           Gi1/0/8, Gi1/0/9, Gi1/0/10
                                           Gi1/0/11, Gi1/0/12, Gi1/0/13
                                           Gi1/0/14, Gi1/0/15, Gi1/0/16
                                           Gi1/0/17, Gi1/0/18, Gi1/0/19
                                           Gi1/0/20, Gi1/0/21, Gi1/0/22
                                           Gi1/0/23, Gi1/0/24, Gi1/0/25
                                           Gi1/0/26, Gi1/0/27, Gi1/0/28
                                           Gi1/0/29, Gi1/0/30, Gi1/0/31
                                           Gi1/0/32, Gi1/0/33, Gi1/0/34
                                           Gi1/0/35, Gi1/0/36, Gi1/0/37
                                           Gi1/0/38, Gi1/0/39, Gi1/0/40
                                           Gi1/0/41, Gi1/0/42, Gi1/0/43
                                           Gi1/0/44, Gi1/0/45, Gi1/0/46
                                           Gi1/0/47, Gi1/0/48
2    VLAN0002              active
40   vlan-40                active
300  VLAN0300              active
1002 fddi-default          act/unsup
1003 token-ring-default  act/unsup
1004 fddinet-default     act/unsup
1005 trnet-default      act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo  Stp  BrdgMode Trans1 Trans2
-----
1    enet  100001    1500  -     -     -        -   -         0     0
2    enet  100002    1500  -     -     -        -   -         0     0
40   enet  100040    1500  -     -     -        -   -         0     0
300  enet  100300    1500  -     -     -        -   -         0     0
1002 fddi  101002    1500  -     -     -        -   -         0     0
1003 tr   101003    1500  -     -     -        -   -         0     0
1004 fdnet 101004    1500  -     -     -        -   -         0     0
1005 trnet 101005    1500  -     -     -        -   -         0     0
2000 enet  102000    1500  -     -     -        -   -         0     0
3000 enet  103000    1500  -     -     -        -   -         0     0

Remote SPAN VLANs
-----
```

2000,3000

```
Primary Secondary Type          Ports
-----
```

Table 61: show vlan Command Output Fields

Field	Description
VLAN	VLAN number.
Name	Name, if configured, of the VLAN.
Status	Status of the VLAN (active or suspend).
Ports	Ports that belong to the VLAN.
Type	Media type of the VLAN.
SAID	Security association ID value for the VLAN.
MTU	Maximum transmission unit size for the VLAN.
Parent	Parent VLAN, if one exists.
RingNo	Ring number for the VLAN, if applicable.
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.
Primary/Secondary/Type/Ports	Includes any private VLANs that have been configured, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it.

This is an example of output from the **show vlan dot1q tag native** command:

```
Device> show vlan dot1q tag native
dot1q native vlan tagging is disabled
```

This is an example of output from the **show vlan private-vlan** command:

```
Device> show vlan private-vlan
Primary Secondary Type          Ports
-----
10      501      isolated      Gi3/0/3
10      502      community     Gi2/0/11
10      503      non-operational3  -
```

```

20    25    isolated    Gi1/0/13, Gi1/0/20, Gi1/0/22, Gi1/0/1, Gi2/0/13, Gi2/0/22,
    Gi3/0/13, Gi3/0/14, Gi3/0/20, Gi3/0/1
20    30    community   Gi1/0/13, Gi1/0/20, Gi1/0/21, Gi1/0/1, Gi2/0/13, Gi2/0/20,
    Gi3/0/14, Gi3/0/20, Gi3/0/21, Gi3/0/1
20    35    community   Gi1/0/13, Gi1/0/20, Gi1/0/23, Gi1/0/33. Gi1/0/1, Gi2/0/13,
    Gi3/0/14, Gi3/0/20. Gi3/0/23, Gi3/0/33, Gi3/0/1
20    55    non-operational
2000  2500   isolated    Gi1/0/5, Gi1/0/10, Gi2/0/5, Gi2/0/10, Gi2/0/15

```

This is an example of output from the **show vlan private-vlan type** command:

```

Device> show vlan private-vlan type
Vlan Type
-----
10    primary
501   isolated
502   community
503   normal

```

This is an example of output from the **show vlan summary** command:

```

Device> show vlan summary
Number of existing VLANs           : 45
Number of existing VTP VLANs      : 45
Number of existing extended VLANs : 0

```

This is an example of output from the **show vlan id** command:

```

Device# show vlan id 2
VLAN Name                Status      Ports
-----
2    VLAN0200              active     Gi1/0/7, Gi1/0/8
2    VLAN0200              active     Gi2/0/1, Gi2/0/2

VLAN Type  SAID      MTU    Parent RingNo BridgeNo Stp    BrdgMode Trans1 Trans2
-----
2    enet  100002   1500   -      -      -      -      -      0      0

Remote SPAN VLANs
-----
Disabled

```

show vmps

To display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, use the **show vmps** command in EXEC mode.

show vmps [**statistics**]

Syntax Description	statistics (Optional) Displays VQP client-side statistics and counters.
---------------------------	--

Command Default	None
------------------------	------

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 vmps** command:

```
Device> show vmps
VQP Client Status:
-----
VMPS VQP Version: 1
Reconfirm Interval: 60 min
Server Retry Count: 3
VMPS domain server:

Reconfirmation status
-----
VMPS Action:          other
```

This is an example of output from the **show vmps statistics** command. The table that follows describes each field in the display.

```
Device> show vmps statistics
VMPS Client Statistics
-----
VQP Queries:          0
VQP Responses:        0
VMPS Changes:         0
VQP Shutdowns:       0
VQP Denied:           0
VQP Wrong Domain:    0
VQP Wrong Version:   0
VQP Insufficient Resource: 0
```

Table 62: show vmmps statistics Field Descriptions

Field	Description
VQP Queries	Number of queries sent by the client to the VMPS.
VQP Responses	Number of responses sent to the client from the VMPS.
VMPS Changes	Number of times that the VMPS changed from one server to another.
VQP Shutdowns	Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively reenable the port to restore connectivity.
VQP Denied	Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period.
VQP Wrong Domain	Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VTP management domain.
VQP Wrong Version	Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS Version 1 requests.
VQP Insufficient Resource	Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached.

show vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the **show vtp** command in EXEC mode.

show vtp {**counters** | **devices** [**conflicts**] | **interface** [*interface-id*] | **password** | **status**}

Syntax Description		
counters		Displays the VTP statistics for the device.
devices		Displays information about all VTP version 3 devices in the domain. This keyword applies only if the device is not running VTP version 3.
conflicts		(Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the device is in VTP transparent or VTP off mode.
interface		Displays VTP status and configuration for all interfaces or the specified interface.
<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 device is running VTP version 3, the display follows these rules:

- If the **password** *password* global configuration command did not specify the **hidden** keyword and encryption is not enabled on the device, the password appears in clear text.
- If the **password** *password* command did not specify the **hidden** keyword and encryption is enabled on the device, the encrypted password appears.
- If the **password** *password* command is included the **hidden** keyword, the hexadecimal secret key is displayed.

This is an example of output from the **show vtp devices** command. A **Yes** in the **Conflict** column indicates that the responding server is in conflict with the local server for the feature; that is, when two devices in the same domain do not have the same primary server for a database.

```
Device# show vtp devices
Retrieving information from the VTP domain. Waiting for 5 seconds.
VTP Database Conf device ID      Primary Server Revision  System Name
      list
-----
VLAN      Yes  00b0.8e50.d000 000c.0412.6300 12354      main.cisco.com
MST       No   00b0.8e50.d000 0004.AB45.6000 24         main.cisco.com
VLAN      Yes  000c.0412.6300=000c.0412.6300 67         qwerty.cisco.com
```

This is an example of output from the **show vtp counters** command. The table that follows describes each field in the display.

```
Device> show vtp counters
VTP statistics:
Summary advertisements received      : 0
Subset advertisements received      : 0
Request advertisements received      : 0
Summary advertisements transmitted  : 0
Subset advertisements transmitted    : 0
Request advertisements transmitted   : 0
Number of config revision errors     : 0
Number of config digest errors       : 0
Number of V1 summary errors          : 0

VTP pruning statistics:

Trunk      Join Transmitted Join Received      Summary advts received from
-----
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 63: show vtp counters Field Descriptions

Field	Description
Summary advertisements received	Number of summary advertisements received by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements received	Number of subset advertisements received by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements received	Number of advertisement requests received by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.

Field	Description
Summary advertisements transmitted	Number of summary advertisements sent by this device on its trunk ports. Summary advertisements contain the management domain name, the configuration revision number, the update timestamp and identity, the authentication checksum, and the number of subset advertisements to follow.
Subset advertisements transmitted	Number of subset advertisements sent by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.
Request advertisements transmitted	Number of advertisement requests sent by this device on its trunk ports. Advertisement requests normally request information on all VLANs. They can also request information on a subset of VLANs.
Number of configuration revision errors	<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 device increments.</p> <p>Revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations.</p> <p>These errors indicate that the device 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 device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same.</p> <p>These errors indicate that the device 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 device in VTP V2 mode receives a VTP Version 1 frame. These errors indicate that at least one neighboring device is either running VTP Version 1 or VTP Version 2 with V2-mode disabled. To solve this problem, change the configuration of the devices in VTP V2-mode to disabled.
Join Transmitted	Number of VTP pruning messages sent on the trunk.
Join Received	Number of VTP pruning messages received on the trunk.
Summary Advts Received from non-pruning-capable device	Number of VTP summary messages received on the trunk from devices that do not support pruning.

This is an example of output from the **show vtp status** command. The table that follows describes each field in the display.

```
Device> show vtp status
VTP Version capable           : 1 to 3
VTP version running           : 1
VTP Domain Name                :
VTP Pruning Mode               : Disabled
VTP Traps Generation           : Disabled
Device ID                      : 2037.06ce.3580
Configuration last modified by 192.168.1.1 at 10-10-12 04:34:02
Local updater ID is 192.168.1.1 on interface LIIN0 (first layer3 interface found
)

Feature VLAN:
-----
VTP Operating Mode             : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs       : 7
Configuration Revision         : 2
MD5 digest                    : 0xA0 0xA1 0xFE 0x4E 0x7E 0x5D 0x97 0x41
                               0x89 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 64: show vtp status Field Descriptions

Field	Description
VTP Version capable	Displays the VTP versions that are capable of operating on the device.
VTP Version running	Displays the VTP version operating on the device. By default, the device implements Version 1 but can be set to Version 2.
VTP Domain Name	Name that identifies the administrative domain for the device.

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 device 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 device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on it. The device guarantees that it can recover all the VLAN information in the current VTP database from NVRAM after reboot. By default, every device is a VTP server.</p> <p>Note The device automatically changes from VTP server mode to VTP client mode if it detects a failure while writing the configuration to NVRAM and cannot return to server mode until the NVRAM is functioning.</p> <p>Client—A device in VTP client mode is enabled for VTP, can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on it. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.</p> <p>Transparent—A device in VTP transparent mode is disabled for VTP, does not send or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received.</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 device.
MD5 Digest	A 16-byte checksum of the VTP configuration.

This is an example of output from the **show vtp status** command for a device running VTP version 3:

```
Device> show vtp status
VTP Version capable : 1 to 3
VTP version running : 3
VTP Domain Name : Cisco
VTP Pruning Mode : Disabled
VTP Traps Generation : Disabled
Device ID : 0021.1bcd.c700

Feature VLAN:
-----
VTP Operating Mode : Server
Number of existing VLANs : 7
Number of existing extended VLANs : 0
Configuration Revision : 0
Primary ID : 0000.0000.0000
Primary Description :
MD5 digest : 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x00 0x00 0x00 0x00 0x00 0x00 0x00 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:
-----
```

switchport mode private-vlan

To configure an interface as either a host private-VLAN port or a promiscuous private-VLAN port, use the **switchport mode private-vlan** 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 private-vlan {host | promiscuous}
no switchport mode private-vlan
```

Syntax Description	host	promiscuous
	Configures the interface as a private-VLAN host port. Host ports belong to private-VLAN secondary VLANs and are either community ports or isolated ports, depending on the VLAN to which they belong.	Configures the interface as a private-VLAN promiscuous port. Promiscuous ports are members of private-VLAN primary VLANs.

Command Default None

Command Modes Interface configuration

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

Usage Guidelines A private-VLAN host or promiscuous port cannot be a Switched Port Analyzer (SPAN) destination port. If you configure a SPAN destination port as a private-VLAN host or promiscuous port, the port becomes inactive.

Do not configure private VLAN on ports with these other features:

- Dynamic-access port VLAN membership
- Dynamic Trunking Protocol (DTP)
- Port Aggregation Protocol (PAgP)
- Link Aggregation Control Protocol (LACP)
- Multicast VLAN Registration (MVR)
- Voice VLAN

While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive

A private-VLAN port cannot be a secure port and should not be configured as a protected port.

For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

We strongly recommend that you enable spanning tree Port Fast and bridge-protocol-data-unit (BPDU) guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence.

If you configure a port as a private-VLAN host port and you do not configure a valid private-VLAN association by using the **switchport private-vlan host-association** command, the interface becomes inactive.

If you configure a port as a private-VLAN promiscuous port and you do not configure a valid private VLAN mapping by using the **switchport private-vlan mapping** command, the interface becomes inactive.

Examples

This example shows how to configure an interface as a private-VLAN host port and associate it to primary VLAN 20. The interface is a member of secondary isolated VLAN 501 and primary VLAN 20.

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode private-vlan host
Device (config-if)# switchport private-vlan host-association 20 501
Device (config-if)# end
```

This example shows how to configure an interface as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode private-vlan promiscuous
Device (config-if)# switchport private-vlan mapping 20 501-503
Device (config-if)# end
```

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 device to send the Cisco Discovery Protocol (CDP) packets to instruct the IP phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You must enable CDP on the device port connected to the Cisco IP Phone to send the configuration to the Cisco IP Phone. (CDP is enabled by default globally and on all device interfaces.)

You should configure voice VLAN on device access ports. You can configure a voice VLAN only on Layer 2 ports.

Before you enable voice VLAN, we recommend that you enable quality of service (QoS) on the interface by entering the **trust device cisco-phone** interface configuration command. If you use the auto QoS feature, these settings are automatically configured.

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport priority extend trust
```

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

switchport trunk

To set the trunk characteristics when the interface is in trunking mode, use the **switchport trunk** command in interface configuration mode. To reset a trunking characteristic to the default, use the **no** form of this command.

```
switchport trunk {allowed vlan vlan-list | native vlan vlan-id | pruning vlan vlan-list}
no switchport trunk {allowed vlan | native vlan | pruning vlan}
```

Syntax Description

allowed vlan <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:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

This example shows how to remove VLANs 3 and 10 to 15 from the pruning-eligible list:


```
Device(config)# interface gigabitethernet1/0/2  
Device(config-if)# switchport trunk pruning vlan remove 3,10-15
```

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

vlan

To add a VLAN and to enter the VLAN configuration mode, use the **vlan** command in global configuration mode. To delete the VLAN, use the **no** form of this command.

vlan *vlan-id*
no vlan *vlan-id*

Syntax Description	<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.				
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 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. With VTP version 1 and 2, extended-range VLANs are not recognized by VTP and are not added to the VLAN database. With VTP version 1 and version 2, before adding extended-range VLANs, you must use the **vtp transparent** global configuration command to put the device in VTP transparent mode. When VTP mode is transparent, VTP mode and domain name and all VLAN configurations are saved in the running configuration, and you can save them in the device startup configuration file.

VTP version 3 supports propagation of extended-range VLANs and you can create them in VTP server or client mode. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

With VTP version 1 and version 2, if you try to create an extended-range VLAN when the device is not in VTP transparent mode, the VLAN is rejected, and you receive an error message.

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 commands that are supported on extended-range VLANs are **mtu** *mtu-size*, **private-vlan**, and **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 device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.

- **ethernet**—Ethernet media type (the default).
- **fd-net**—FDDI network entity title (NET) media type.
- **fdi**—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.

- **mtu** *mtu-size*—Specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 576 to 18190. The default is 1500 bytes.
- **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.
- **private-vlan**—Configures the VLAN as a private VLAN community, isolated, or primary VLAN or configures the association between private VLAN primary and secondary VLANs. For more information, see the **private-vlan** command.
- **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.
- **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 65: 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> , mtu <i>mtu-size</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> , mtu <i>mtu-size</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> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee 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> , mtu <i>mtu-size</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> , mtu <i>mtu-size</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> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee 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> , mtu <i>mtu-size</i> , bridge <i>bridge-number</i> , stp type {ieee 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 66: 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:

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```

This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vtp mode transparent
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

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

vlan dot1q tag native

To enable tagging of native VLAN frames on all IEEE 802.1Q trunk ports, use the **vlan dot1q tag native** command in global configuration mode. To return to the default setting, use the **no** form of this command.

```
vlan dot1q tag native
no vlan dot1q tag native
```

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.

You can use this command with the IEEE 802.1Q tunneling feature. This feature operates on an edge device of a service-provider network and expands VLAN space by using a VLAN-in-VLAN hierarchy and tagging the tagged packets. You must use IEEE 802.1Q trunk ports for sending packets to the service-provider network. However, packets going through the core of the service-provider network might also be carried on IEEE 802.1Q trunks. If the native VLANs of an IEEE 802.1Q trunk match the native VLAN of a tunneling port on the same device, traffic on the native VLAN is not tagged on the sending trunk port. This command ensures that native VLAN packets on all IEEE 802.1Q trunk ports are tagged.

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

You can verify your settings by entering the **show vlan dot1q tag native** privileged EXEC command.

vmps reconfirm (global configuration)

To change the reconfirmation interval for the VLAN Query Protocol (VQP) client, use the **vmps reconfirm** global configuration command. To return to the default setting, use the **no** form of this command.

vmps reconfirm *interval*
no vmps reconfirm

Syntax Description	<i>interval</i> Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes.				
Command Default	The default reconfirmation interval is 60 minutes.				
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	You can verify your setting by entering the show vmps privileged EXEC command and examining information in the Reconfirm Interval row.				
Examples	<p>This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:</p> <pre>Device(config)# vmps reconfirm 20</pre>				

vmps reconfirm (privileged EXEC)

To immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS), use the **vmps reconfirm** privileged EXEC command.

vmps reconfirm

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 You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

Examples This example shows how to immediately send VQP queries to the VMPS:

```
Device# vmps reconfirm
```

vmps retry

To configure the per-server retry count for the VLAN Query Protocol (VQP) client, use the **vmps retry** command in global configuration mode. Use the **no** form of this command to return to the default setting.

```
vmps retry count
no vmps retry
```

Syntax Description	<i>count</i> Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10.				
Command Default	The default retry count is 3.				
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 set the retry count to 7:

```
Device(config)# vmps retry 7
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

vmps server

To configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers, use the **vmps server** command in global configuration mode. Use the **no** form of this command to remove a VMPS server.

```
vmps server {hostname|ip address} [primary]
no vmps server {hostname|ip address} [primary]
```

Syntax Description	
<i>hostname</i>	Hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured.
<i>ip address</i>	IP address of the primary or secondary VMPS servers.
primary	(Optional) Decides whether primary or secondary VMPS servers are being configured.

Command Default No primary or secondary VMPS servers are defined.

Command Modes Global configuration

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

Usage Guidelines The first server entered is automatically selected as the primary server whether or not primary is entered. The first server address can be overridden by using primary in a subsequent command.

If a member device in a cluster configuration does not have an IP address, the cluster does not use the VMPS server configured for that member device. Instead, the cluster uses the VMPS server on the command device, and the command device proxies the VMPS requests. The VMPS server treats the cluster as a single device and uses the IP address of the command device to respond to requests.

When using the **no** form without specifying the IP address, all configured servers are deleted. If you delete all servers when dynamic access ports are present, the device cannot forward packets from new sources on these ports because it cannot query the VMPS.

This example shows how to configure the server with IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Device(config)# vmps server 191.10.49.20 primary
Device(config)# vmps server 191.10.49.21
Device(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Device(config)# no vmps server 191.10.49.21
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the VMPS Domain Server row.

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 device. 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 device in VTP client mode. A device in VTP client mode is enabled for VTP, and can send advertisements, but does not have enough nonvolatile storage to store VLAN configurations. You cannot configure VLANs on a VTP client. VLANs are configured on another device in the domain that is in server mode. When a VTP client starts up, it does not send VTP advertisements until it receives advertisements to initialize its VLAN database.	
off	Places the device in VTP off mode. A device in VTP off mode functions the same as a VTP transparent device except that it does not forward VTP advertisements on trunk ports.	
server	Places the device in VTP server mode. A device in VTP server mode is enabled for VTP and sends advertisements. You can configure VLANs on the device. The device can recover all the VLAN information in the current VTP database from nonvolatile storage after reboot.	
transparent	Places the device in VTP transparent mode. A device in VTP transparent mode is disabled for VTP, does not send advertisements or learn from advertisements sent by other devices, and cannot affect VLAN configurations on other devices in the network. The device receives VTP advertisements and forwards them on all trunk ports except the one on which the advertisement was received. When VTP mode is transparent, the mode and domain name are saved in the device running configuration file, and you can save them in the device startup configuration file by entering the copy running-config startup config privileged EXEC command.	
mst	(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).	

unknown	(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).
vlan	(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).
password <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 device.
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 device startup configuration file and reboot the device, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.
- Domain names are case-sensitive.
- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device to VTP server mode.
- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the device is not in client or transparent mode.
- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in server mode or transparent mode, the device configuration is not changed.
- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.
- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.
- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.
- In VTP Versions 1 and 2, the VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file. VTP supports extended-range VLANs in client and server mode and saves them in the VLAN database.
- With VTP Versions 1 and 2, if extended-range VLANs are configured on the device and you attempt to set the VTP mode to server or client, you receive an error message, and the configuration is not allowed. Changing VTP mode is allowed with extended VLANs in VTP Version 3.
- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.
- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.
- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.

- When you use the **no vtp password** form of the command, the device returns to the no-password state.
- The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

- VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.
- If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.
- Only VLANs in the pruning-eligible list can be pruned.
- Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

- Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.
- Each VTP device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.
- If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices in the VTP domain.
- If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.
- If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.
- If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.
- In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.
- Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Device(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Device(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Device(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the device:


```
Device(config)# vtp domain OurDomainName
```

This example shows how to place the device in VTP transparent mode:

```
Device(config)# vtp mode transparent
```

This example shows how to configure the VTP domain password:

```
Device(config)# vtp password ThisIsOurDomainsPassword
```

This example shows how to enable pruning in the VLAN database:

```
Device(config)# vtp pruning  
Pruning switched ON
```

This example shows how to enable Version 2 mode in the VLAN database:

```
Device(config)# vtp version 2
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.

vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the **vtp** command in interface configuration mode. To disable VTP on the interface, use the **no** form of this command.

vtp
no vtp

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Interface configuration

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

Usage Guidelines Enter this command only on interfaces that are in trunking mode.

This command is supported only when the device is running VTP Version 3.

This example shows how to enable VTP on an interface:

```
Device(config-if)# vtp
```

This example shows how to disable VTP on an interface:

```
Device(config-if)# no vtp
```

vtp primary

To configure a device as the VLAN Trunking Protocol (VTP) primary server, use the **vtp primary** command in privileged EXEC mode.

```
vtp primary [{mst | vlan}] [force]
```

Syntax Description	Parameter	Description
	mst	(Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature.
	vlan	(Optional) Configures the device as the primary VTP server for VLANs.
	force	(Optional) Configures the device to not check for conflicting devices when configuring the primary server.

Command Default The device is a VTP secondary server.

Command Modes Privileged EXEC

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

Usage Guidelines A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to NVRAM.

By default, all devices come up as secondary servers. Primary server status is needed only for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers.

Primary server status is lost if the device reloads or domain parameters change.



Note This command is supported only when the device is running VTP Version 3.

This example shows how to configure the device as the primary VTP server for VLANs:

```
Device# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

You can verify your settings by entering the **show vtp status** privileged EXEC command.



INDEX

A

access-session mac-move deny command [686](#)
action command [689](#)
arp command [891](#)
authentication mac-move permit command [692](#)
authentication priority command [694](#)
auto qos classify command [568](#)
auto qos trust command [574](#)
auto qos video command [582](#)
auto qos voip command [593](#)
available power [53](#)

B

boot command [892](#)
budgeted power [53](#)

C

cache command [381](#)
cache-memory-max command [211](#)
cat command [893](#)
channel-group command [277](#)
channel-protocol command [280](#)
Cisco Discovery Protocol (CDP) [1046](#)
cisp enable [699](#)
class command [610](#)
class-map command [613](#)
clear errdisable interface vlan [700](#)
clear ip mfib command [212](#)
clear ip mroute command [213](#)
clear l2protocol-tunnel counters command [1008](#)
clear lacp command [281](#)
clear location command [894](#)
clear location statistics command [895](#)
clear mac address-table command [701](#)
clear pagp command [282](#)
clear spanning-tree counters command [283](#)
clear spanning-tree detected-protocols command [284](#)
clear vmps statistics command [1009](#)
clear vtp counters command [1010](#)
collect command [387](#)
collect counter command [388](#)
collect interface command [389](#)

collect timestamp absolute command [390](#)
collect transport tcp flags command [391](#)
consumed power [53](#)
copy command [896](#)

D

datalink flow monitor command [392](#)
debug auto qos command [606](#)
debug etherchannel command [285](#)
debug flow exporter command [393](#)
debug flow monitor command [394](#)
debug ilpower command [31](#)
debug interface command [32](#)
debug lacp command [286](#)
debug lldp packets command [33](#)
debug pagp command [287](#)
debug platform pm command [288](#)
debug platform poe command [34](#)
debug platform stack-manager command [840](#)
debug platform udd command [290](#)
debug platform vlan command [1011](#)
debug spanning-tree command [291](#)
debug sw-vlan command [1012](#)
debug sw-vlan ifs command [1014](#)
debug sw-vlan notification command [1015](#)
debug sw-vlan vtp command [1016](#)
delete command [900](#)
deny command [710](#)
description command [397](#)
destination command [398](#)
dir command [901](#)
dot1x supplicant force-multicast command [722](#)
dot1x test timeout [724](#)
dscp command [399](#)
duplex command [35](#)

E

emergency-install command [903](#)
epm access-control open command [727](#)
errdisable detect cause command [37](#)
errdisable recovery cause command [39](#)
errdisable recovery interval command [42](#)

exit command [905](#)
 export-protocol netflow-v9 command [400](#)

F

flash_init command [906](#)
 flow-based RSPAN (FRSPAN) session [481](#)
 flow-based SPAN (FSPAN) session [481](#)
 full-ring state [866](#)

H

help command [907](#)

I

interface command [43](#)
 interface port-channel command [293](#)
 interface vlan command [1018](#)
 ip admission name command [730](#)
 ip device tracking maximum command [732](#)
 ip device tracking probe command [733](#)
 ip dhcp snooping verify no-relay-agent-address [737](#)
 ip flow monitor command [405](#)
 ip igmp snooping last-member-query-count command [219](#)
 ip mtu command [47](#)
 ip multicast auto-enable command [226](#)
 ip verify source command [743](#)
 ipv6 flow monitor command [269, 407](#)
 ipv6 mtu command [48](#)

L

l2protocol-tunnel command [1019](#)
 l2protocol-tunnel cos command [1022](#)
 lACP max-bundle command [294](#)
 lACP port-priority command [295](#)
 lACP system-priority command [297](#)
 license right-to-use [909](#)
 lldp (interface configuration) command [49](#)
 location plm calibrating command [914](#)
 logging event power-inline-status command [51](#)

M

mab request format attribute 32 command [749](#)
 mac address-table move update command [915](#)
 main-cpu command [841](#)
 match (access-map configuration) command [752](#)
 match (class-map configuration) command [615](#)
 match datalink dot1q priority command [409](#)
 match datalink dot1q vlan command [410](#)
 match datalink ethernet type command [411](#)
 match datalink mac command [412](#)
 match datalink vlan command [413](#)

match flow direction command [415](#)
 match interface command [416](#)
 match ipv4 command [417](#)
 match ipv4 destination address command [418](#)
 match ipv4 source address command [419](#)
 match ipv4 ttl command [420](#)
 match ipv6 command [421](#)
 match ipv6 destination address command [422](#)
 match ipv6 hop-limit command [423](#)
 match ipv6 source command [424](#)
 match non-client-nrt command [618](#)
 match transport command [425](#)
 match transport icmp ipv4 command [426](#)
 match transport icmp ipv6 command [427](#)
 maximum transmission unit (MTU) [121, 129](#)
 mdix auto command [52](#)
 mgmt_init command [916](#)
 mkdir command [917](#)
 mode (power-stack configuration) command [53](#)
 mode command [428](#)
 monitor session command [475, 477](#)
 monitor session filter command [481](#)
 monitor session source command [483](#)
 more command [918](#)

N

network-policy command [55](#)
 network-policy configuration mode [56](#)
 network-policy profile (global configuration) command [56](#)
 network-policy profiles [95](#)
 no authentication logging verbose [757](#)
 no dot1x logging verbose [758](#)
 no mab logging verbose [759](#)

O

option command [429](#)

P

pagp learn-method command [298](#)
 pagp port-priority command [300](#)
 partial-ring state [866](#)
 permit command [760](#)
 persistent MAC address [863](#)
 policy config-sync prc reload command [843](#)
 policy-map command [619](#)
 port-channel auto command [302](#)
 port-channel load-balance command [303](#)
 port-channel load-balance extended command [305](#)
 port-channel min-links command [306](#)
 power efficient-ethernet auto command [57](#)
 power inline command [60](#)
 power inline police command [64](#)

power stack configuration mode **53**
 power supply command **66**
 power-priority command **58**
 private-vlan command **1023**
 private-vlan mapping command **1025**

Q

queue-limit command **624**

R

real-time power consumption policing **64**
 redistribute mdns-sd command **239**
 redundancy command **844**
 redundancy config-sync mismatched-commands command **845**
 redundancy force-switchover command **847**
 redundancy reload command **848**
 reload command **849**
 Remote SPAN (RSPAN) sessions **491, 495**
 rename command **920**
 request platform software console attach switch command **921**
 request platform software trace archive **1001, 1002**
 request platform software trace filter binary **1003**
 reset command **945**
 rmdir command **946**
 RSPAN **475, 477, 481, 483**
 sessions **475, 477, 483**
 add interfaces to **475, 477, 483**
 start new **475, 477, 483**

S

sdm prefer command **947**
 security passthru command **772**
 service-list mdns-sd service-list-name command **240**
 service-policy command **243, 626**
 service-policy-query command **241**
 service-routing mdns-sd command **242**
 session command **851**
 set command **628, 948**
 set platform software trace **990, 994**
 show auto qos command **607**
 show avc client command **951**
 show cable-diagnostics tdr command **952**
 show cisp command **788**
 show class-map command **634**
 show dot1q-tunnel command **1027**
 show eap command **792**
 show eee command **68**
 show env command **71, 955**
 show env xps command **957**
 show errdisable detect command **74**
 show errdisable recovery command **75**
 show etherchannel command **317**

show flow exporter command **433**
 show flow record command **442**
 show interfaces command **76**
 show interfaces counters command **80**
 show interfaces private-vlan mapping command **1028**
 show interfaces switchport command **82**
 show interfaces transceiver command **84**
 show ip pim autorp command **253**
 show ip pim bsr command **255**
 show ip pim bsr-router command **254**
 show ip pim tunnel command **256**
 show ip sla statistics command **488**
 show l2protocol-tunnel command **1029**
 show lacp command **321**
 show license right-to-use command **966**
 show location command **968**
 show mac address-table move update command **969**
 show macsec command **796**
 show mgmt-infra trace messages ilpower command **91**
 show mgmt-infra trace messages ilpower-ha command **93**
 show mgmt-infra trace messages platform-mgr-poe command **94**
 show mka policy command **798**
 show mka session command **801**
 show mka statistics command **804**
 show mka summary command **807**
 show mod command **90**
 show monitor command **491**
 show monitor session command **495**
 show network-policy profile command **95**
 show pagp command **325**
 show platform etherchannel command **327**
 show platform ip wccp command **499**
 show platform pm command **328**
 show platform software fed active ip multicast command **262**
 show platform software fed active ip wccp command **497**
 show platform software fed switch ip multicast command **262**
 show platform software fed switch ip wccp command **497**
 show platform software trace level **998**
 show platform software trace message **995**
 show platform stack-manager command **852**
 show platform vlan command **1031**
 show policy-map command **642**
 show power inline command **113**
 show redundancy command **853**
 show redundancy config-sync command **857**
 show sampler command **443**
 show sdm prefer command **973**
 show stack-power command **119**
 show storm-control **812**
 show switch command **859**
 show system mtu command **121**
 show tech-support command **122**
 show uddl command **331**
 show vlan access-map command **814**
 show vlan command **1032**
 show vlan filter command **815**

- show vlan group command [816](#)
 - show vmps command [1036](#)
 - show vtp command [1038](#)
 - snmp-server enable traps bridge command [505](#)
 - snmp-server enable traps bulkstat command [506](#)
 - snmp-server enable traps call-home command [507](#)
 - snmp-server enable traps cef command [508](#)
 - snmp-server enable traps command [502](#)
 - snmp-server enable traps CPU command [509](#)
 - snmp-server enable traps envmon command [510](#)
 - snmp-server enable traps errdisable command [511](#)
 - snmp-server enable traps flash command [512](#)
 - snmp-server enable traps isis command [513](#)
 - snmp-server enable traps license command [514](#)
 - snmp-server enable traps mac-notification command [515](#)
 - snmp-server enable traps ospf command [516](#)
 - snmp-server enable traps pim command [517](#)
 - snmp-server enable traps port-security command [518](#)
 - snmp-server enable traps power-ethernet command [519](#)
 - snmp-server enable traps snmp command [520](#)
 - snmp-server enable traps stackwise command [521](#)
 - snmp-server enable traps storm-control command [523](#)
 - snmp-server enable traps stpx command [524](#)
 - snmp-server enable traps transceiver command [525](#)
 - snmp-server enable traps vrfmib command [526](#)
 - snmp-server enable traps vstack command [527](#)
 - snmp-server engineID command [528](#)
 - snmp-server host command [529](#)
 - speed command [124](#)
 - stack member number [870](#)
 - stack member priority [867](#)
 - stack-mac persistent timer command [863](#)
 - stack-mac update force command [864](#)
 - stack-power command [126](#)
 - StackPower [119, 126](#)
 - standby console enable command [865](#)
 - storm-control command [817](#)
 - switch priority command [867](#)
 - switch provision command [868](#)
 - switch renumber command [870](#)
 - switch stack port command [866](#)
 - Switched Port Analyzer (SPAN) sessions [491, 495](#)
 - switchport access vlan command [336](#)
 - switchport block command [128](#)
 - switchport command [334](#)
 - switchport mode access [534, 535](#)
 - switchport mode command [339](#)
 - switchport mode private-vlan command [1044](#)
 - switchport nonegotiate command [341](#)
 - switchport port-security aging command [820](#)
 - switchport port-security mac-address command [822](#)
 - switchport port-security maximum command [824](#)
 - switchport port-security violation command [826](#)
 - switchport priority extend command [1046](#)
 - switchport trunk command [1047](#)
 - switchport voice vlan command [342](#)
 - system env temperature threshold yellow command [975](#)
 - system mtu command [129](#)
- ## T
- template data timeout command [447](#)
 - test cable-diagnostics tdr command [977](#)
 - test mcu read register command [130](#)
 - traceroute mac command [978](#)
 - traceroute mac ip command [981](#)
 - transport command [448](#)
 - ttl command [449](#)
 - type command [983](#)
- ## U
- udld command [345](#)
 - udld port command [347](#)
 - udld reset command [349](#)
 - unset command [984](#)
- ## V
- version command [986](#)
 - vlan access-map command [832](#)
 - vlan command [1050](#)
 - vlan dot1q tag native command [1056](#)
 - vlan filter command [834](#)
 - vlan group command [835](#)
 - vmps reconfirm (global configuration) command [1057](#)
 - vmps reconfirm (privileged EXEC) command [1058](#)
 - vmps retry command [1059](#)
 - vmps server command [1060](#)
 - voice vlan command [134](#)
 - voice-signaling vlan command [132](#)
 - vtp (global configuration) command [1061](#)
 - vtp (interface configuration) command [1066](#)
 - vtp primary command [1067](#)

Notices

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

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

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

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

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

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

