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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS.

CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

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

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

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

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 1
Cisco TrustSec 13

CHAPTER 2
Cisco TrustSec Commands 15
cts authorization list 16
cts change-password 17
cts credentials 18
cts refresh  20
cts rekey  22
ccts role-based enforcement  23
ccts role-based l2-vrf  24
ccts role-based monitor  26
ccts role-based permissions  27
ccts role-based sgt-caching  29
ccts role-based sgt-map  30
ccts xsp connection peer  32
ccts xsp default password  35
ccts xsp default source-ip  37
ccts xsp filter-enable  39
ccts xsp filter-group  40
ccts xsp filter-list  42
ccts xsp log binding-changes  44
ccts xsp reconciliation period  45
ccts xsp retry period  46
propagate sgt (cts manual)  47
sap mode-list (cts manual)  49
show ccts credentials  51
show ccts interface  52
show ccts role-based counters  54
show ccts role-based permissions  56
show ccts server-list  58
show ccts xsp  59

P A R T  I I
High Availability  63

C H A P T E R  3
High Availability Commands  65
  clear diagnostic event-log  67
  diagnostic monitor  68
  diagnostic schedule module  70
  diagnostic start  73
  diagnostic stop  76
domain id 78
dual-active detection pagp 79
dual-active recovery-reload-disable 80
hw-module beacon switch 81
hw-module switch slot 82
hw-module switch usbflash 84
main-cpu 85
maintenance-template 86
mode sso 87
policy config-sync prc reload 88
redundancy 89
reload 90
router routing protocol shutdown l2 92
set platform software fed switch 93
set platform software nif-mgr switch 94
show diagnostic bootup 95
show diagnostic content 96
show diagnostic description 100
show diagnostic events 102
show diagnostic result 104
show diagnostic simulation failure 109
show diagnostic schedule 110
show hw-module switch subslot 111
show logging onboard switch 113
show platform software fed 116
show platform software nif-mgr switch 119
show redundancy 123
show redundancy config-sync 127
show stackwise-virtual 129
show tech-support stack 131
stackwise-virtual 136
stackwise-virtual dual-active-detection 137
stackwise-virtual link 138
standby console enable 139
PART III

Interface and Hardware Components

CHAPTER 4

Interface and Hardware Commands

- start maintenance 140
- stop maintenance 141
- system mode maintenance 142

- bluetooth pin 147
- debug ilpower 148
- debug interface 149
- debug lldp packets 150
- debug platform poe 151
- debug platform software fed switch active punt packet-capture start 152
- duplex 153
- enable (interface configuration) 155
- errdisable detect cause 156
- errdisable recovery cause 158
- errdisable recovery cause 160
- interface 162
- interface range 164
- ip mtu 166
- ipv6 mtu 167
- lldp (interface configuration) 168
- mode (power-stack configuration) 170
- network-policy 172
- network-policy profile (global configuration) 173
- power-priority 174
- power supply 176
- shell trigger 178
- show beacon all 179
- show env 180
- show errdisable detect 183
- show errdisable recovery 185
- show interfaces 186
show interfaces counters 189
show interfaces switchport 191
show interfaces transceiver 193
show inventory 197
show memory platform 203
show module 206
show mgmt-infra trace messages ilpower 207
show mgmt-infra trace messages ilpower-ha 209
show mgmt-infra trace messages platform-mgr-poe 210
show network-policy profile 211
show platform hardware bluetooth 212
show platform hardware capacity 213
show platform hardware fed switch forward 225
show platform hardware fed switch forward interface 228
show platform hardware fed switch forward last summary 231
show platform resources 234
show platform software audit 235
show platform software fed switch punt cpuq rates 239
show platform software fed switch punt packet-capture display 241
show platform software fed switch punt rates interfaces 243
show platform software ilpower 246
show platform software memory 248
show platform software process list 253
show platform software process memory 257
show platform software process slot switch 260
show platform software status control-processor 262
show platform software thread list 265
show processes cpu platform 267
show processes cpu platform history 270
show processes cpu platform monitor 273
show processes memory platform 275
show processes platform 279
show system mtu 282
show tech-support 283
show tech-support bgp 285
show tech-support diagnostic 288
show tech-support poe 290
speed 305
switchport block 307
system mtu 308

voice-signaling vlan (network-policy configuration) 309
voice vlan (network-policy configuration) 311

PART IV

IP Addressing Services 313

CHAPTER 5

IP Addressing Services Commands 315

clear ip nhrp 320
clear ipv6 access-list 321
clear ipv6 dhcp 322
clear ipv6 dhcp binding 323
clear ipv6 dhcp client 324
clear ipv6 dhcp conflict 325
clear ipv6 dhcp relay binding 326
clear ipv6 eigrp 327
clear ipv6 mfib counters 328
clear ipv6 mld counters 329
clear ipv6 mld traffic 330
clear ipv6 mtu 331
clear ipv6 multicast aaa authorization 332
clear ipv6 nd destination 333
clear ipv6 nd on-link prefix 334
clear ipv6 nd router 335
clear ipv6 neighbors 336
clear ipv6 nhrp 338
clear ipv6 ospf 339
clear ipv6 ospf counters 340
clear ipv6 ospf events 342
clear ipv6 pim reset 343
clear ipv6 pim topology 344
clear ipv6 pim traffic 345
clear ipv6 prefix-list 346
clear ipv6 rip 347
clear ipv6 route 348
clear ipv6 spd 349
debug nhrp 350
fhrp delay 352
fhrp version vrrp v3 353
ip address dhcp 354
ip address pool (DHCP) 357
ip address 358
ip nhrp authentication 361
ip nhrp holdtime 362
ip nhrp map 363
ip nhrp map multicast 365
ip nhrp network-id 366
ip nhrp nhs 367
ip nhrp registration 369
ipv6 access-list 370
ipv6 address-validate 373
ipv6 cef 374
ipv6 cef accounting 376
ipv6 cef distributed 378
ipv6 cef load-sharing algorithm 380
ipv6 cef optimize neighbor resolution 381
ipv6 destination-guard policy 382
ipv6 dhcp-relay bulk-lease 383
ipv6 dhcp-relay option vpn 384
ipv6 dhcp-relay source-interface 385
ipv6 dhcp binding track ppp 386
ipv6 dhcp database 387
ipv6 dhcp iana-route-add 389
ipv6 dhcp iapd-route-add 390
ipv6 source-guard attach-policy 436
ipv6 source-route 437
ipv6 spd mode 438
ipv6 spd queue max-threshold 440
ipv6 traffic interface-statistics 441
ipv6 unicast-routing 442
key chain 443
key-string (authentication) 444
key 445
show ip nrp nhs 446
show ip ports all 448
show ipv6 access-list 450
show ipv6 destination-guard policy 453
show ipv6 dhcp 454
show ipv6 dhcp binding 455
show ipv6 dhcp conflict 458
show ipv6 dhcp database 459
show ipv6 dhcp guard policy 461
show ipv6 dhcp interface 463
show ipv6 dhcp relay binding 465
show ipv6 eigrp events 467
show ipv6 eigrp interfaces 469
show ipv6 eigrp topology 471
show ipv6 eigrp traffic 473
show ipv6 general-prefix 475
show ipv6 interface 476
show ipv6 mib 484
show ipv6 mld groups 490
show ipv6 mld interface 493
show ipv6 mld snooping 495
show ipv6 mld ssm-map 497
show ipv6 mld traffic 499
show ipv6 mrib client 501
show ipv6 mrib route 503
show ipv6 mroute 505
show ipv6 mtu 509
show ipv6 nd destination 511
show ipv6 nd on-link prefix 512
show ipv6 neighbors 513
show ipv6 nhrp 517
show ipv6 ospf 520
show ipv6 ospf border-routers 524
show ipv6 ospf event 526
show ipv6 ospf graceful-restart 529
show ipv6 ospf interface 531
show ipv6 ospf request-list 536
show ipv6 ospf request-list 538
show ipv6 ospf retransmission-list 540
show ipv6 ospf summary-prefix 542
show ipv6 ospf timers rate-limit 543
show ipv6 ospf traffic 544
show ipv6 ospf virtual-links 548
show ipv6 pim anycast-RP 550
show ipv6 pim bsr 551
show ipv6 pim df 553
show ipv6 pim group-map 555
show ipv6 pim interface 557
show ipv6 pim join-prune statistic 559
show ipv6 pim limit 560
show ipv6 pim neighbor 561
show ipv6 pim range-list 563
show ipv6 pim topology 565
show ipv6 pim traffic 567
show ipv6 pim tunnel 569
show ipv6 policy 571
show ipv6 prefix-list 572
show ipv6 protocols 575
show ipv6 rip 578
show ipv6 route 583
show ipv6 routers 587
show ipv6 rpf 590
show ipv6 source-guard policy 592
show ipv6 spd 593
show ipv6 static 594
show ipv6 traffic 598
show key chain 601
show track 602
track 604
vrrp 606
vrrp description 607
vrrp preempt 608
vrrp priority 609
vrrp timers advertise 610
vrrs leader 612

PART V

IP Multicast Routing 613

CHAPTER 6

IP Multicast Routing Commands 615

clear ip mfib counters 617
clear ip mroute 618
clear ip pim snooping vlan 619
ip igmp filter 620
ip igmp max-groups 621
ip igmp profile 623
ip igmp snooping 624
ip igmp snooping last-member-query-count 625
ip igmp snooping querier 627
ip igmp snooping report-suppression 629
ip igmp snooping vlan mrouter 630
ip igmp snooping vlan static 631
ip multicast auto-enable 632
ip multicast-routing 633
CHAPTER 7

Layer 2/3 Commands 683
avb 685
avb vlan 686
channel-group 687
channel-protocol 690
clear lacp 691
clear pagp 692
clear spanning-tree counters 693
clear spanning-tree detected-protocols 694
debug etherchannel 695
debug lacp 696
debug pagp 697
debug platform pm 698
debug platform uddl 699
debug spanning-tree 700
interface port-channel 702
lacp max-bundle 704
lacp port-priority 705
lacp rate 706
lacp system-priority 707
no ptp enable 708
pagp learn-method 709
pagp port-priority 711
policy-map 712
port-channel 714
port-channel auto 715
port-channel load-balance 716
port-channel load-balance extended 719
port-channel min-links 720
ptp priority1 value 721
ptp priority2 value 722
ptp profile dot1as 723
mvrp vlan creation 724
mvrp registration 725
mvrp timer 727
rep admin vlan 729
rep block port 730
rep lsl-age-timer 732
rep lsl-retries 733
rep preempt delay 734
rep preempt segment 735
rep segment 736
rep stcn 738
show avb domain 739
show avb streams 741
show etherchannel 742
show interfaces rep detail 745
show lacp 746
show msrp port bandwidth 750
show msrp streams 752
show pagp 754
show platform etherchannel 756
show platform hardware fed active vlan ingress 757
show platform pm 758
show platform software fed switch ptp 759
show ptp brief 761
show ptp clock 762
show ptp parent 763
show ptp port 764
show rep topology 765
show uddl 767
show vlan dot1q tag native 771
switchport 772
switchport access vlan 773
switchport mode 774
switchport nonegotiate 776
switchport trunk 777
switchport voice vlan 780
udld 783
udld fast-hello 785
udld port 786
udld reset 788
vtp mode 789

PART VII

Multiprotocol Label Switching 791

CHAPTER 8

MPLS Commands 793
backup peer 794
encapsulation mpls 795
l2vpn xconnect context 796
load-balance 797
member pseudowire 799
mpls label range 801
mpls label protocol (interface configuration) 804
mpls label protocol (global configuration) 805
mpls ip (interface configuration) 806
mpls ip (global configuration) 807
mpls ip default-route 808
neighbor (MPLS) 809
tunnel destination 810
tunnel mode gre multipoint 811
tunnel source 812
show ip pim mdt send 814
show ip pim mdt receive 815
show ip pim mdt history 817
show ip pim mdt bgp 818
ip pim sparse-mode 819
ip pim nbma-mode 820
mdt log-reuse 821
mdt default 822
mdt data 824
snmp-server enable traps vrfmib  921
snmp-server enable traps vstack  922
snmp-server engineID  923
snmp-server group  924
snmp-server host  928
snmp-server user  933
snmp-server view  937
source (ERSPAN)  939
switchport mode access  940
switchport voice vlan  941

PART IX  QoS  943

CHAPTER 10  QoS Commands  945
  auto qos classify  946
  auto qos trust  948
  auto qos video  955
  auto qos voip  965
  class  979
  class-map  981
  debug auto qos  983
  match (class-map configuration)  984
  policy-map  988
  priority  990
  queue-buffers ratio  992
  queue-limit  993
  random-detect cos  995
  random-detect cos-based  996
  random-detect dscp  997
  random-detect dscp-based  999
  random-detect precedence  1000
  random-detect precedence-based  1002
  service-policy (Wired)  1003
  set  1005
show auto qos 1011
show class-map 1013
show platform hardware fed switch 1014
show platform software fed switch qos 1018
show platform software fed switch qos qsb 1019
show policy-map 1022
show tech-support qos 1024
trust device 1026

PART X  1029

CHAPTER 11  1031

IP Routing Commands  1031

address-family ipv6 (OSPF) 1033
aggregate-address 1034
area nssa 1037
area virtual-link 1039
auto-summary (BGP) 1042
authentication (BFD) 1045
bfd 1046
bfd all-interfaces 1048
bfd check-ctrl-plane-failure 1049
bfd echo 1050
bfd slow-timers 1052
bfd template 1054
bfd-template single-hop 1055
bgp graceful-restart 1056
clear proximity ip bgp 1058
default-information originate (OSPF) 1062
default-metric (BGP) 1064
distance (OSPF) 1066
eigrp log-neighbor-changes 1069
ip authentication key-chain eigrp 1071
ip authentication mode eigrp 1072
ip bandwidth-percent eigrp 1073
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip cef load-sharing algorithm</td>
<td>1074</td>
</tr>
<tr>
<td>ip community-list</td>
<td>1075</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>1080</td>
</tr>
<tr>
<td>ip hello-interval eigrp</td>
<td>1083</td>
</tr>
<tr>
<td>ip hold-time eigrp</td>
<td>1084</td>
</tr>
<tr>
<td>ip load-sharing</td>
<td>1085</td>
</tr>
<tr>
<td>ip next-hop-self eigrp</td>
<td>1086</td>
</tr>
<tr>
<td>ip ospf database-filter all out</td>
<td>1088</td>
</tr>
<tr>
<td>ip ospf name-lookup</td>
<td>1089</td>
</tr>
<tr>
<td>ip split-horizon eigrp</td>
<td>1090</td>
</tr>
<tr>
<td>ip summary-address eigrp</td>
<td>1091</td>
</tr>
<tr>
<td>ip route static bfd</td>
<td>1093</td>
</tr>
<tr>
<td>ipv6 route static bfd</td>
<td>1095</td>
</tr>
<tr>
<td>metric weights (EIGRP)</td>
<td>1096</td>
</tr>
<tr>
<td>neighbor advertisement-interval</td>
<td>1098</td>
</tr>
<tr>
<td>neighbor default-originate</td>
<td>1100</td>
</tr>
<tr>
<td>neighbor description</td>
<td>1102</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>1103</td>
</tr>
<tr>
<td>neighbor maximum-prefix (BGP)</td>
<td>1104</td>
</tr>
<tr>
<td>neighbor peer-group (assigning members)</td>
<td>1106</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>1108</td>
</tr>
<tr>
<td>neighbor route-map</td>
<td>1111</td>
</tr>
<tr>
<td>neighbor update-source</td>
<td>1113</td>
</tr>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>1115</td>
</tr>
<tr>
<td>network (EIGRP)</td>
<td>1117</td>
</tr>
<tr>
<td>nsf (EIGRP)</td>
<td>1119</td>
</tr>
<tr>
<td>offset-list (EIGRP)</td>
<td>1121</td>
</tr>
<tr>
<td>router bgp</td>
<td>1123</td>
</tr>
<tr>
<td>router-id</td>
<td>1126</td>
</tr>
<tr>
<td>router eigrp</td>
<td>1127</td>
</tr>
<tr>
<td>redistribute (IPv6)</td>
<td>1128</td>
</tr>
<tr>
<td>redistribute maximum-prefix (OSPF)</td>
<td>1131</td>
</tr>
<tr>
<td>rewrite-evpn-rt-asn</td>
<td>1133</td>
</tr>
<tr>
<td>router ospf</td>
<td>1134</td>
</tr>
</tbody>
</table>
PART XI

CHAPTER 12

Security 1213

aaa accounting 1218
aaa accounting dot1x 1221
aaa accounting identity 1223
aaa authentication dot1x 1225
aaa authorization 1226
aaa new-model 1230
authentication host-mode 1232
authentication logging verbose 1234
authentication mac-move permit 1235
authentication priority 1237
authentication violation 1240
cisp enable 1242
clear errdisable interface vlan 1243
clear mac address-table 1244
deny (MAC access-list configuration) 1246
device-role (IPv6 snooping) 1250
device-role (IPv6 nd inspection) 1251
device-tracking policy 1252
dot1x critical (global configuration) 1254
dot1x logging verbose 1255
dot1x max-start 1256
dot1x pae 1257
dot1x supplicant controlled transient 1258
dot1x supplicant force-multicast 1259
dot1x test eapol-capable 1260
dot1x test timeout 1261
dot1x timeout 1262
dtls 1264
enable password 1266
enable secret 1269
epm access-control open 1272
ip access-list role-based 1273
ip admission 1274
ip admission name 1275
ip dhcp snooping database 1277
ip dhcp snooping information option format remote-id 1279
ip dhcp snooping verify no-relay-agent-address 1280
ip http access-class 1281
ip radius source-interface 1283
ip source binding 1285
ip ssh source-interface 1286
ip verify source 1287
ipv6 access-list 1288
ipv6 snooping policy 1290
key chain macsec 1291
key config-key password-encrypt 1292
limit address-count 1294
PART XII  
System Management  1383

CHAPTER 13  
System Management Commands  1385

arp  1387
boot  1388
cat  1389
copy  1390

copy startup-config tftp:  1391
copy tftp: startup-config  1392
debug voice diagnostics mac-address  1393
debug platform condition feature multicast controlplane  1394
debug platform condition mac  1396
debug ilpower powerman  1398
delete  1401
dir  1402
emergency-install  1404
exit  1406
factory-reset  1407
flash_init  1408
help  1409
install  1410
l2 traceroute  1414
license boot level  1415
license smart deregister  1417
license smart register idtoken  1418
license smart renew  1419
location  1420
location plm calibrating  1423
mac address-table move update  1424
mgmt_init  1425
mkdir  1426
more  1427
no debug all  1428
rename  1429
request consent-token accept-response shell-access  1430
request consent-token generate-challenge shell-access  1431
request consent-token terminate-auth  1432
request platform software console attach switch  1433
reset  1435
rmdir  1436
sdm prefer  1437
service private-config-encryption  1438
set  1439
show avc client  1442
show debug  1443
show env  1444
show env xps  1446
show flow monitor  1450
show install  1452
show license all  1454
show license status  1456
show license summary  1458
show license udi  1459
show license usage  1460
show location  1461
show logging onboard switch uptime  1463
CHAPTER 14

Tracing 1535

Information About Tracing 1536

Tracing Overview 1536

Location of Tracelogs 1536

TraceLog Naming Convention 1536

Rotation and Throttling Policy 1537

Tracing Levels 1537

set platform software trace 1538
show platform software trace filter-binary 1542
show platform software trace message 1543
show platform software trace level 1546
request platform software trace archive 1549
request platform software trace rotate all 1550
request platform software trace filter-binary 1551

PART XIII

CHAPTER 15

VLAN Commands 1555

clear vtp counters 1556
debug sw-vlan 1557
debug sw-vlan ifs 1558
debug sw-vlan notification 1559
debug sw-vlan vtp 1560
dot1q vlan native 1562
interface (VLAN) 1563
private-vlan 1564
private-vlan mapping 1566
show dot1q-tunnel 1568
show interfaces private-vlan mapping 1569
show vlan 1570
show vtp 1574
switchport mode private-vlan 1580
switchport priority extend 1582
switchport trunk 1583
vlan 1586
vlan dot1q tag native 1592
vtp (global configuration) 1593
vtp (interface configuration) 1598
vtp primary 1599
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

<table>
<thead>
<tr>
<th>Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
<th>About This Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Begin a session with your switch.</td>
<td>Switch&gt;</td>
<td>Enter <strong>logout</strong> or <strong>quit</strong>.</td>
<td>Use this mode to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Change terminal settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Perform basic tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Display system information.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>While in user EXEC mode, enter the <strong>enable</strong> command.</td>
<td>Device#</td>
<td>Enter <strong>disable</strong> to exit.</td>
<td>Use this mode to verify commands that you have entered. Use a password to protect access to this mode.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>While in privileged EXEC mode, enter the <strong>configure</strong> command.</td>
<td>Device(config)#</td>
<td>To exit to privileged EXEC mode, enter <strong>exit</strong> or <strong>end</strong>, or press Ctrl-Z.</td>
<td>Use this mode to configure parameters that apply to the entire switch.</td>
</tr>
<tr>
<td>Mode</td>
<td>Access Method</td>
<td>Prompt</td>
<td>Exit Method</td>
<td>About This Mode</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>VLAN configuration</td>
<td>While in global configuration mode, enter the <strong>vlan vlan-id</strong> command.</td>
<td><strong>Device(config-vlan)#</strong></td>
<td>To exit to global configuration mode, enter the <strong>exit</strong> command.</td>
<td>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.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>While in global configuration mode, enter the <strong>interface</strong> command (with a specific interface).</td>
<td><strong>Device(config-if)#</strong></td>
<td>To exit to global configuration mode, enter <strong>exit</strong>.</td>
<td>Use this mode to configure parameters for the Ethernet ports.</td>
</tr>
<tr>
<td>Line configuration</td>
<td>While in global configuration mode, specify a line with the <strong>line vty</strong> or <strong>line console</strong> command.</td>
<td><strong>Device(config-line)#</strong></td>
<td>To exit to global configuration mode, enter <strong>exit</strong>.</td>
<td>Use this mode to configure parameters for the terminal line.</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>help</strong></td>
<td>Obtains a brief description of the help system in any command mode.</td>
</tr>
<tr>
<td><strong>abbreviated-command-entry ?</strong></td>
<td>Obtains a list of commands that begin with a particular character string.</td>
</tr>
</tbody>
</table>

Device# di?
dir disable disconnect
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

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Meaning</th>
<th>How to Get Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Ambiguous command: &quot;show con&quot;</td>
<td>You did not enter enough characters for your switch to recognize the command.</td>
<td>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.</td>
</tr>
<tr>
<td>% Incomplete command.</td>
<td>You did not enter all the keywords or values required by this command.</td>
<td>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.</td>
</tr>
<tr>
<td>% Invalid input detected at `^' marker.</td>
<td>You entered the command incorrectly. The caret (^) marks the point of the error.</td>
<td>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.</td>
</tr>
</tbody>
</table>

### 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.

<table>
<thead>
<tr>
<th>Action</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press Ctrl-P or the up arrow key.</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Press Ctrl-N or the down arrow key.</td>
<td>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.</td>
</tr>
<tr>
<td>show history</td>
<td>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.</td>
</tr>
<tr>
<td>Device(config)# help</td>
<td></td>
</tr>
</tbody>
</table>

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.

---

**Table 5: Editing Commands through Keystrokes**

<table>
<thead>
<tr>
<th>Capability</th>
<th>Keystroke</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move around the command line to</td>
<td>Press Ctrl-B, or press the</td>
<td>Moves the cursor back one character.</td>
</tr>
<tr>
<td>make changes or corrections.</td>
<td>left arrow key.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-F, or press the</td>
<td>Moves the cursor forward one character.</td>
</tr>
<tr>
<td></td>
<td>right arrow key.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-A.</td>
<td>Moves the cursor to the beginning of the command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>line.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-E.</td>
<td>Moves the cursor to the end of the command line.</td>
</tr>
<tr>
<td></td>
<td>Press Esc B.</td>
<td>Moves the cursor back one word.</td>
</tr>
<tr>
<td></td>
<td>Press Esc F.</td>
<td>Moves the cursor forward one word.</td>
</tr>
<tr>
<td></td>
<td>Press Ctrl-T.</td>
<td>Transposes the character to the left of the cursor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with the character located at the cursor.</td>
</tr>
<tr>
<td>Capability</td>
<td>Keystroke</td>
<td>Purpose</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recall commands from the buffer and paste them in the command line.</td>
<td>Press Ctrl-Y.</td>
<td>Recalls the most recent entry in the buffer.</td>
</tr>
<tr>
<td>The switch provides a buffer with the last ten items that you deleted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Press Esc Y.</td>
<td></td>
<td>Recalls the next buffer entry.</td>
</tr>
<tr>
<td>The buffer contains only the last 10 items that you have deleted or cut.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>If you press Esc Y more than ten times, you cycle to the first buffer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>entry.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete entries if you make a mistake or change your mind.</td>
<td>Press the <strong>Delete</strong> or <strong>Backspace</strong> key.</td>
<td>Erases the character to the left of the cursor.</td>
</tr>
<tr>
<td>Press Ctrl-D.</td>
<td></td>
<td>Deletes the character at the cursor.</td>
</tr>
<tr>
<td>Press Ctrl-K.</td>
<td></td>
<td>Deletes all characters from the cursor to the end of the command line.</td>
</tr>
<tr>
<td>Press Ctrl-U or Ctrl-X.</td>
<td></td>
<td>Deletes all characters from the cursor to the beginning of the command line.</td>
</tr>
<tr>
<td>Press Ctrl-W.</td>
<td></td>
<td>Deletes the word to the left of the cursor.</td>
</tr>
<tr>
<td>Press Esc D.</td>
<td></td>
<td>Deletes from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Capitalize or lowercase words or capitalize a set of letters.</td>
<td>Press Esc C.</td>
<td>Capitalizes at the cursor.</td>
</tr>
<tr>
<td>Press Esc L.</td>
<td></td>
<td>Changes the word at the cursor to lowercase.</td>
</tr>
<tr>
<td>Press Esc U.</td>
<td></td>
<td>Capitalizes letters from the cursor to the end of the word.</td>
</tr>
<tr>
<td>Designate a particular keystroke as an executable command, perhaps as a</td>
<td>Press Ctrl-V or Esc Q.</td>
<td></td>
</tr>
<tr>
<td>shortcut.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
Device(config)# access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 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 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
Device(config)# $ access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
Device(config)# $ access-list 101 permit tcp 131.108.2.5 255.255.255.0 131.108.1.20 255.255.255.0 eq 45
```

---

#### Capability Keystroke Purpose

<table>
<thead>
<tr>
<th>Scroll down a line or screen on displays that are longer than the terminal screen can display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press the <strong>Return</strong> key.</td>
</tr>
</tbody>
</table>

**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 **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. |
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.
Using the Command-Line Interface

Accessing the CLI through a Console Connection or through Telnet
PART I

Cisco TrustSec

• Cisco TrustSec Commands, on page 15
Cisco TrustSec Commands

- `cts authorization list`, on page 16
- `cts change-password`, on page 17
- `cts credentials`, on page 18
- `cts refresh`, on page 20
- `cts rekey`, on page 22
- `cts role-based enforcement`, on page 23
- `cts role-based l2-vrf`, on page 24
- `cts role-based monitor`, on page 26
- `cts role-based permissions`, on page 27
- `cts role-based sgt-caching`, on page 29
- `cts role-based sgt-map`, on page 30
- `cts xvp connection peer`, on page 32
- `cts xvp default password`, on page 35
- `cts xvp default source-ip`, on page 37
- `cts xvp filter-enable`, on page 39
- `cts xvp filter-group`, on page 40
- `cts xvp filter-list`, on page 42
- `cts xvp log binding-changes`, on page 44
- `cts xvp reconciliation period`, on page 45
- `cts xvp retry period`, on page 46
- `propagate sgt (cts manual)`, on page 47
- `sap mode-list (cts manual)`, on page 49
- `show cts credentials`, on page 51
- `show cts interface`, on page 52
- `show cts role-based counters`, on page 54
- `show cts role-based permissions`, on page 56
- `show cts server-list`, on page 58
- `show cts xvp`, on page 59
cts authorization list

To specify a list of authentication, authorization, and accounting (AAA) servers to be used by the TrustSec seed device, use the `cts authorization list` command on the Cisco TrustSec seed device in global configuration mode. Use the `no` form of the command to stop using the list during authentication.

```plaintext
cts authorization list server_list

no cts authorization list server_list
```

**Syntax Description**

- `server_list` Cisco TrustSec AAA server group.

**Command Default**

None

**Command Modes**

Global configuration (config)

**Supported User Roles**

Administrator

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This command is only for the seed device. Non-seed devices obtain the TrustSec AAA server list from their TrustSec authenticator peer as a component of their TrustSec environment data.

The following example displays an AAA configuration of a TrustSec seed device:

```plaintext
Device# cts credentials id Device1 password Cisco123
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# aaa authorization network MLIST group radius
Device(config)# cts authorization list MLIST
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# radius-server host 10.20.3.1 auth-port 1812 acct-port 1813 pac key AbCe1234
Device(config)# radius-server vsa send authentication
Device(config)# dot1x system-auth-control
Device(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cts server-list</td>
<td>Displays RADIUS server configurations.</td>
</tr>
</tbody>
</table>
cts change-password

To change the password between the local device and the authentication server, use the `cts change-password` privileged EXEC command.

```
cts change-password server ipv4_address udp_port {a-id hex_string | key radius_key} [{source interface_list}]
```

**Syntax Description**

- `server` Specifies the authentication server.
- `ipv4_address` IP address of the authentication server.
- `udp_port` UDP port of the authentication server.
- `a-id hex_string` Specifies the identification string of the ACS server.
- `key` Specifies the RADIUS key to be used for provisioning.
- `source interface_list` (Optional) Specifies the interface type and its identifying parameters as per the displayed list for source address in request packets.

**Command Default**

None.

**Command Modes**

Privileged EXEC (#)

**Supported User Roles**

Administrator

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `cts change-password` command allows an administrator to change the password used between the local device and the Cisco Secure ACS authentication server, without having to reconfigure the authentication server.

The following example shows how to change the Cisco TrustSec password between a switch and a Cisco Secure ACS:

```
Device# cts change-password server 192.168.2.2 88 a-id ffe
```
**cts credentials**

Use the **cts credentials** command in privileged EXEC mode to specify the TrustSec ID and password of the network device. Use the **clear cts credentials** command to delete the credentials.

```
certs credentials id  cts_id  password  cts_pwd
```

**Syntax Description**

- **credentials id  cts_id** Specifies the Cisco TrustSec device ID for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The *cts-id* variable has a maximum length of 32 characters and is case sensitive.

- **password  cts_pwd** Specifies the password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Supported User Roles**

Administrator

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **cts credentials** command specifies the Cisco TrustSec device ID and password for this device to use when authenticating with other Cisco TrustSec devices with EAP-FAST. The Cisco TrustSec credentials state retrieval is not performed by the nonvolatile generation process (NVGEN) because the Cisco TrustSec credential information is saved in the keystore, and not in the startup configuration. The device can be assigned a Cisco TrustSec identity by the Cisco Secure Access Control Server (ACS), or a new password auto-generated when prompted to do so by the ACS. These credentials are stored in the keystore, eliminating the need to save the running configuration. To display the Cisco TrustSec device ID, use the **show cts credentials** command. The stored password is never displayed.

To change the device ID or the password, reenter the command. To clear the keystore, use the **clear cts credentials** command.

**Note**

When the Cisco TrustSec device ID is changed, all Protected Access Credentials (PACs) are flushed from the keystore because PACs are associated with the old device ID and are not valid for a new identity.

The following example shows how to configure the Cisco TrustSec device ID and password:

```
Device# cts credentials id cts1 password password1
```

CTS device ID and password have been inserted in the local keystore. Please make sure that the same ID and password are configured in the server database.
The following example show how to change the Cisco TrustSec device ID and password to cts_new and password123, respectively:

Device# cts credentials id cts_new password password123
A different device ID is being configured.
This may disrupt connectivity on your CTS links.
Are you sure you want to change the Device ID? [confirm] y

TS device ID and password have been inserted in the local keystore. Please make sure that the same ID and password are configured in the server database.

The following sample output displays the Cisco TrustSec device ID and password state:

Device# show cts credentials

CTS password is defined in keystore, device-id - cts_new

---

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cts credentials</td>
<td>Clears the Cisco TrustSec device ID and password.</td>
</tr>
<tr>
<td>show cts credentials</td>
<td>Displays the state of the current Cisco TrustSec device ID and password.</td>
</tr>
<tr>
<td>show cts keystore</td>
<td>Displays contents of the hardware and software keystores.</td>
</tr>
</tbody>
</table>
## cts refresh

To refresh the TrustSec peer authorization policy of all or specific Cisco TrustSec peers, or to refresh the SGACL policies downloaded to the device by the authentication server, use the `cts refresh` command in privileged EXEC mode.

### Syntax

```
cts refresh [peer [peer_id] | sgt [{sgt_number | default | unknown}]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Environment-data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>environment-data</code></td>
<td>Refreshes environment data.</td>
</tr>
</tbody>
</table>

| `peer Peer-ID` | (Optional) If a peer-id is specified, only policies related to the specified peer connection are refreshed. |

| `sgt sgt_number` | (Optional) Performs an immediate refresh of the SGACL policies from the authentication server. |

  * If an SGT number is specified, only policies related to that SGT are refreshed. |

| `default` | (Optional) Refreshes the default SGACL policy. |

| `unknown` | (Optional) Refreshes the unknown SGACL policy. |

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Supported User Roles

Administrator

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To refresh the Peer Authorization Policy on all TrustSec peers, enter `cts policy refresh` without specifying a peer ID.

The peer authorization policy is initially downloaded from the Cisco ACS at the end of the EAP-FAST NDAC authentication success. The Cisco ACS is configured to refresh the peer authorization policy, but the `cts policy refresh` command can force immediate refresh of the policy before the Cisco ACS timer expires. This command is relevant only to TrustSec devices that can impose Security Group Tags (SGTs) and enforce Security Group Access Control Lists (SGACLs).

The following example shows how to refresh the TrustSec peer authorization policy of all peers:

```
Device# cts policy refresh
Policy refresh in progress
```

The following sample output displays the TrustSec peer authorization policy of all peers:

```
VSS-1# show cts policy peer
```
CTS Peer Policy

device-id of the peer that this local device is connected to
Peer name: VSS-2T-1
Peer SGT: 1-02
Trusted Peer: TRUE
Peer Policy Lifetime = 120 secs
Peer Last update time = 12:19:09 UTC Wed Nov 18 2009
Policy expires in 0:00:01:51 (dd:hr:mm:sec)
Policy refreshes in 0:00:01:51 (dd:hr:mm:sec)
Cache data applied = NONE

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear cts policy</td>
<td>Clears all Cisco TrustSec policies, or by the peer ID or SGT.</td>
</tr>
<tr>
<td>show cts policy peer</td>
<td>Displays peer authorization policy for all or specific TrustSec peers.</td>
</tr>
</tbody>
</table>
cts rekey

To regenerate the Pairwise Master Key used by the Security Association Protocol (SAP), use the `cts rekey` privileged EXEC command.

```
ccts rekey interface type slot/port
```

**Syntax Description**

- `interface type slot/port` Specifies the Cisco TrustSec interface on which to regenerate the SAP key.

**Command Default**

None.

**Command Modes**

Privileged EXEC (#)

**Supported User Roles**

Administrator

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

SAP Pair-wise Master Key key (PMK) refresh ordinarily occurs automatically, triggered by combinations of network events and non-configurable internal timers related to dot1X authentication. The ability to manually refresh encryption keys is often part of network administration security requirements. To manually force a PMK refresh, use the `cts rekey` command.

TrustSec supports a manual configuration mode where dot1X authentication is not required to create link-to-link encryption between switches. In this case, the PMK is manually configured on devices on both ends of the link with the `sap pmk` Cisco TrustSec manual interface configuration command.

The following example shows how to regenerate the PMK on a specified interface:

```
Device# cts rekey interface gigabitEthernet 2/1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap mode-list (cts manual)</td>
<td>Configures Cisco TrustSec SAP for manual mode.</td>
</tr>
</tbody>
</table>
cts role-based enforcement

To enable role-based access control globally and on specific Layer 3 interfaces using Cisco TrustSec, use the `cts role-based enforcement` command in global configuration mode and interface configuration mode respectively. To disable the enforcement of role-based access control at an interface level, use the `no` form of this command.

```
cts role-based enforcement
no cts role-based enforcement
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Enforcement of role-based access control at an interface level is disabled globally.

**Command Modes**

- Global configuration (config)
- Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Fuji 16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `cts role-based enforcement` command in global configuration mode enables role-based access control globally. Once role-based access control is enabled globally, it is automatically enabled on every Layer 3 interface on the device. To disable role-based access control on specific Layer 3 interfaces, use the `no` form of the command in interface configuration mode. The `cts role-based enforcement` command in interface configuration mode enables enforcement of role-based access control on specific Layer 3 interfaces.

The attribute-based access control list organizes and manages the Cisco TrustSec access control on a network device. The security group access control list (SGACL) is a Layer 3-4 access control list to filter access based on the value of the security group tag (SGT). The filtering usually occurs at an egress port of the Cisco TrustSec domain. The terms role-based access control list (RBACL) and SGACL can be used interchangeably, and they refer to a topology-independent ACL used in an attribute-based access control (ABAC) policy model.

The following example shows how to enable role-based access control on a Gigabit Ethernet interface:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/1/3
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```
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} [{,}] [{-}]
nob cts role-based l2-vrf vrf-name vlan-list {all vlan-ID} [{,}] [{-}]
```

**Syntax Description**

- **vrf-name**: Name of the VRF instance.
- **vlan-list**: Specifies the list of VLANs to be assigned to a VRF instance.
- **all**: Specifies all VLANs.
- **vlan-ID**: 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(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:

```
Device(config)# interface vlan 101
Device(config-if)# vrf forwarding vrf1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface vlan</td>
<td>Configures a VLAN interface.</td>
</tr>
<tr>
<td>vrf forwarding</td>
<td>Associates a VRF instance or a virtual network with an interface or subinterface.</td>
</tr>
<tr>
<td>show cts role-based permissions</td>
<td>Displays the SGACL permission list.</td>
</tr>
</tbody>
</table>
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.

```plaintext
cts role-based monitor {all | permissions {default [{ipv4 | ipv6}] | from {sgt | unknown} to {sgt | unknown} [{ipv4 | ipv6}]}}
no cts role-based monitor {all | permissions {default [{ipv4 | ipv6}] | from {sgt | unknown} to {sgt | unknown} [{ipv4 | ipv6}]}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Monitors permissions for all source tags to all destination tags.</td>
</tr>
<tr>
<td><code>permissions</code></td>
<td>Monitors permissions from a source tags to a destination tags.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Monitors the default permission list.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Specifies the IPv4 protocol.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Specifies the IPv6 protocol.</td>
</tr>
<tr>
<td><code>from</code></td>
<td>Specifies the source group tag for filtered traffic.</td>
</tr>
<tr>
<td><code>sgt</code></td>
<td>Security Group Tag (SGT). Valid values are from 2 to 65519.</td>
</tr>
<tr>
<td><code>unknown</code></td>
<td>Specifies an unknown source or destination group tag (DST).</td>
</tr>
</tbody>
</table>

### Command Default

Role-based access control monitoring is not enabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```
Device(config)# cts role-based monitor permissions from 10 to 11
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cts role-based permissions</code></td>
<td>Displays the SGACL permission list.</td>
</tr>
</tbody>
</table>
# 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.

```plaintext
cts role-based permissions {default | from {sgt | unknown} to {sgt | unknown}} {rbacl-name | ipv4 | ipv6}
no cts role-based permissions {default | from {sgt | unknown} to {sgt | unknown}} {rbacl-name | ipv4 | ipv6}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>from</strong></td>
<td>Specifies the source group tag of the filtered traffic.</td>
</tr>
<tr>
<td><strong>sgt</strong></td>
<td>Security Group Tag (SGT). Valid values are from 2 to 65519.</td>
</tr>
<tr>
<td><strong>unknown</strong></td>
<td>Specifies an unknown source or destination group tag.</td>
</tr>
<tr>
<td><strong>rbacl-name</strong></td>
<td>Role-based access control list (RBACL) or SGACL name. Up to 16 SGACLs can be specified in the configuration.</td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
<td>Specifies the IPv4 protocol.</td>
</tr>
<tr>
<td><strong>ipv6</strong></td>
<td>Specifies the IPv6 protocol.</td>
</tr>
</tbody>
</table>

## Command Default

Permissions from a source group to a destination group is not enabled.

## Command Modes

Global configuration (config)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## 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:

```plaintext
Device(config)# cts role-based permissions from 6 to 6 mon_2
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show cts role-based permissions</code></td>
<td>Displays the SGACL permission list.</td>
</tr>
</tbody>
</table>
**cts role-based sgt-caching**

To enable Security Group Tag (SGT) caching globally, use the `cts role-based sgt-caching` command in global configuration mode. To remove SGT caching, use the `no` form of this command.

```
ccts role-based sgt-caching [vlan-list {vlan-id | all}]
no cts role-based sgt-caching [vlan-list {vlan-id | all}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-list vlan-id</code></td>
<td>(Optional) Specifies VLAN IDs. Individual VLAN IDs are separated by commas, and a range of IDs specified with a hyphen. Valid values are from 1 to 4094.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Selects all VLANs.</td>
</tr>
</tbody>
</table>

**Command Default**

SGT caching is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To enable SGT caching on a VLAN, both `cts role-based sgt-caching` and `cts role-based sgt-caching vlan-list` commands must be configured.

**Example**

The following example shows how to enable SGT caching on a VLAN:

```
Device# configure terminal
Device(config)# cts role-based sgt-caching
Device(config)# cts role-based sgt-caching vlan-list 4
```
# cts role-based sgt-map

To manually map a source IP address to a Security Group Tag (SGT) on either a host or a VRF, use the `cts role-based sgt-map` command in global configuration mode. Use the `no` form of the command to remove the mapping.

```plaintext
cts role-based sgt-map  {ipv4_netaddress | ipv6_netaddress | ipv4_netaddress/prefix | ipv6_netaddress/prefix} sgt sgt-number
cts role-based sgt-map host  {ipv4_hostaddress | ipv6_hostaddress} sgt sgt-number
cts role-based sgt-map vlan-list  {vlan_ids | all} sgt sgt-number
cts role-based sgt-map vrf instance_name
    {ipv4_netaddress | ipv6_netaddress | ipv4_netaddress/prefix | ipv6_netaddress/prefix | host
     {ipv4_hostaddress | ipv6_hostaddress}} sgt sgt-number
no cts role-based sgt-map
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv4_netaddress</code></td>
<td>IPv4 address in dot decimal notation.</td>
</tr>
<tr>
<td><code>ipv6_netaddress</code></td>
<td>IPv6 address in colon hexadecimal notation.</td>
</tr>
<tr>
<td><code>ipv4_netaddress/prefix</code></td>
<td>Maps the SGT to all hosts of the specified subnet address (IPv4 or IPv6). IPv4 is specified in dot decimal CIDR notation, IPv6 in colon hexadecimal notation.</td>
</tr>
<tr>
<td><code>ipv6_netaddress/prefix</code></td>
<td></td>
</tr>
<tr>
<td><code>host</code></td>
<td>Binds the specified host IP address with the SGT. Enter the IPv4 address in dot decimal notation; IPv6 in colon hexadecimal notation.</td>
</tr>
<tr>
<td><code>vlan-list</code></td>
<td>Specifies VLAN IDs.</td>
</tr>
<tr>
<td><code>vlan_ids</code></td>
<td>Individual VLAN IDs are separated by commas, a range of IDs specified with a hyphen.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Specifies all VLAN IDs.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>Specifies a VRF instance, previously created on the device.</td>
</tr>
<tr>
<td><code>instance_name</code></td>
<td></td>
</tr>
<tr>
<td><code>sgt</code></td>
<td>Specifies the SGT number from 0 to 65,535.</td>
</tr>
<tr>
<td><code>sgt-number</code></td>
<td></td>
</tr>
</tbody>
</table>

## Command Default

None

## Command Modes

Global configuration (config)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

If you do not have a Cisco Identity Services Engine, Cisco Secure ACS, dynamic Address Resolution Protocol (ARP) inspection, Dynamic Host Control Protocol (DHCP) snooping, or Host Tracking available on your
device to automatically map SGTs to source IP addresses, you can manually map an SGT to the following with the **cts role-based sgt-map** command:

- A single host IPv4 or IPv6 address
- All hosts of an IPv4 or IPv6 network or subnetwork
- VRFs
- Single or multiple VLANs

The **cts role-based sgt-map** command binds the specified SGT with packets that fall within the specified network address.

SXP exports an exhaustive expansion of all possible individual IP-SGT bindings within the specified network or subnetwork. IPv6 bindings and subnet bindings are exported only to SXP listener peers of SXP version 2 or later. The expansion does not include host bindings which are known individually or are configured or learnt from SXP for any nested subnet bindings.

The **cts role-based sgt-map host** command binds the specified SGT with incoming packets when the IP source address is matched by the specified host address. This IP-SGT binding has the lowest priority and is ignored in the presence of any other dynamically discovered bindings from other sources (such as, SXP or locally authenticated hosts). The binding is used locally on the device for SGT imposition and SGACL enforcement. It is exported to SXP peers if it is the only binding known for the specified host IP address.

The **vrf** keyword specifies a virtual routing and forwarding table previously defined with the vrf definition global configuration command. The IP-SGT binding specified with the **cts role-based sgt-map vrf** global configuration command is entered into the IP-SGT table associated with the specified VRF and the IP protocol version which is implied by the type of IP address entered.

The **cts role-based sgt-map vlan-list** command binds an SGT with a specified VLAN or a set of VLANs. The keyword **all** is equivalent to the full range of VLANs supported by the device and is not preserved in the nonvolatile generation (NVGEN) process. The specified SGT is bound to incoming packets received in any of the specified VLANs. The system uses discovery methods such as DHCP and/or ARP snooping (a.k.a. IP device tracking) to discover active hosts in any of the VLANs mapped by this command. Alternatively, the system could map the subnet associated with the SVI of each VLAN to the specified SGT. SXP exports the resulting bindings as appropriate for the type of binding.

### Examples

The following example shows how to manually map a source IP address to an SGT:

```
Device(config)# cts role-based sgt-map 10.10.1.1 sgt 77
```

In the following example, a device binds host IP address 10.1.2.1 to SGT 3 and 10.1.2.2 to SGT 4. These bindings are forwarded by SXP to an SGACL enforcement device.

```
Device(config)# cts role-based sgt-map host 10.1.2.1 sgt 3
Device(config)# cts role-based sgt-map host 10.1.2.2 sgt 4
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show cts role-based sgt-map</td>
<td>Displays role-based access control information.</td>
</tr>
</tbody>
</table>
cts sxp connection peer

To enter the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) peer IP address, to specify if a password is used for the peer connection, to specify the global hold-time period for a listener or speaker device, and to specify if the connection is bidirectional, use the cts sxp connection peer command in global configuration mode. To remove these configurations for a peer connection, use the no form of this command.

cts sxp connection peer ipv4-address {source | password} {default | none} mode {local | peer} [{[[{listener | speaker}]]} [{hold-time minimum-time maximum-time | vrf vrf-name}]] | both [vrf vrf-name]]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4-address</td>
<td>SXP peer IPv4 address.</td>
</tr>
<tr>
<td>source</td>
<td>Specifies the source IPv4 address.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies that an SXP password is used for the peer connection.</td>
</tr>
<tr>
<td>default</td>
<td>Specifies that the default SXP password is used.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no password is used.</td>
</tr>
<tr>
<td>mode</td>
<td>Specifies either the local or peer SXP connection mode.</td>
</tr>
<tr>
<td>local</td>
<td>Specifies that the SXP connection mode refers to the local device.</td>
</tr>
<tr>
<td>peer</td>
<td>Specifies that the SXP connection mode refers to the peer device.</td>
</tr>
<tr>
<td>listener</td>
<td>(Optional) Specifies that the device is the listener in the connection.</td>
</tr>
<tr>
<td>speaker</td>
<td>(Optional) Specifies that the device is the speaker in the connection.</td>
</tr>
<tr>
<td>hold-time minimum-time maximum-time</td>
<td>(Optional) Specifies the hold-time period, in seconds, for the device. The range for minimum and maximum time is from 0 to 65535. A maximum-time value is required only when you use the following keywords: peer speaker and local listener. In other instances, only a minimum-time value is required.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies the virtual routing and forwarding (VRF) instance name to the peer.</td>
</tr>
<tr>
<td>both</td>
<td>(Optional) Specifies that the device is both the speaker and the listener in the bidirectional SXP connection.</td>
</tr>
</tbody>
</table>
The CTS-SXP peer IP address is not configured and no CTS-SXP peer password is used for the peer connection. The default setting for a CTS-SXP connection password is **none**.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When a CTS-SXP connection to a peer is configured with the `cts sxp connection peer` command, only the connection mode can be changed. The `vrf` keyword is optional. If a VRF name is not provided or a VRF name is provided with the `default` keyword, then the connection is set up in the default routing or forwarding domain.

A **hold-time maximum-period** value is required only when you use the following keywords: **peer speaker** and **local listener**. In other instances, only a **hold-time minimum-period** value is required.

---

**Note**

The **maximum-period** value must be greater than or equal to the **minimum-period** value.

Use the **both** keyword to configure a bidirectional SXP connection. With the support for bidirectional SXP configuration, a peer can act as both a speaker and a listener and propagate SXP bindings in both directions using a single connection.

**Examples**

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B> enable
Device_B# configure terminal
Device_B#(config)# cts sxp enable
Device_B#(config)# cts sxp default password Cisco123
Device_B#(config)# cts sxp default source-ip 10.20.2.2
Device_B#(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```

You can also configure both peer and source IP addresses for an SXP connection. The source IP address specified in the `cts sxp connection` command overwrites the default value.

```
Device_A(config)# cts sxp connection peer 51.51.51.1 source 51.51.51.2 password none mode local speaker
```
Device_B(config)# cts sxp connection peer 51.51.51.2 source 51.51.51.1 password none mode local listener

The following example shows how to enable bidirectional CTS-SXP and configure the SXP peer connection on Device_A to connect to Device_B:

Device_A> enable
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local both

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts sxp default password</td>
<td>Configures the Cisco TrustSec SXP default password.</td>
</tr>
<tr>
<td>cts sxp default source-ip</td>
<td>Configures the Cisco TrustSec SXP source IPv4 address.</td>
</tr>
<tr>
<td>cts sxp enable</td>
<td>Enables Cisco TrustSec SXP on a device.</td>
</tr>
<tr>
<td>cts sxp log</td>
<td>Enables logging for IP-to-SGT binding changes.</td>
</tr>
<tr>
<td>cts sxp reconciliation</td>
<td>Changes the Cisco TrustSec SXP reconciliation period.</td>
</tr>
<tr>
<td>cts sxp retry</td>
<td>Changes the Cisco TrustSec SXP retry period timer.</td>
</tr>
<tr>
<td>cts sxp speaker hold-time</td>
<td>Configures the global hold-time period of a speaker device in a Cisco TrustSec SGT SXPv4 network.</td>
</tr>
<tr>
<td>cts sxp listener hold-time</td>
<td>Configures the global hold-time period of a listener device in a Cisco TrustSec SGT SXPv4 network.</td>
</tr>
<tr>
<td>show cts sxp</td>
<td>Displays the status of all Cisco TrustSec SXP configurations.</td>
</tr>
</tbody>
</table>
cts sxp default password

To specify the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) default password, use the `cts sxp default password` command in global configuration mode. To remove the CTS-SXP default password, use the `no` form of this command.

**Syntax**

```plaintext
ccts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-key cleartext-pwd}
no ccts sxp default password {0 unencrypted-pwd | 6 encrypted-key | 7 encrypted-key cleartext-pwd}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 unencrypted-pwd</td>
<td>Specifies that an unencrypted CTS-SXP default password follows. The maximum password length is 32 characters.</td>
</tr>
<tr>
<td>6 encrypted-key</td>
<td>Specifies that a 6 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.</td>
</tr>
<tr>
<td>7 encrypted-key</td>
<td>Specifies that a 7 encryption type password is used as the CTS-SXP default password. The maximum password length is 32 characters.</td>
</tr>
<tr>
<td>cleartext-pwd</td>
<td>Specifies a cleartext CTS-SXP default password. The maximum password length is 32 characters.</td>
</tr>
</tbody>
</table>

**Command Default**

Type 0 (cleartext)

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `cts sxp default password` command sets the CTS-SXP default password to be optionally used for all CTS-SXP connections configured on the device. The CTS-SXP password can be cleartext, or encrypted with the 0, 7, 6 encryption type keywords. If the encryption type is 0, then an unencrypted cleartext password follows.

**Examples**

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A# configure terminal
Device_A#(config)# cts sxp enable
Device_A#(config)# cts sxp default password Cisco123
Device_A#(config)# cts sxp default source-ip 10.10.1.1
Device_A#(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B# configure terminal
```
cts sxp default password

Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts sxp connection peer</td>
<td>Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.</td>
</tr>
<tr>
<td>cts sxp default source-ip</td>
<td>Configures the CTS-SXP source IPv4 address.</td>
</tr>
<tr>
<td>cts sxp enable</td>
<td>Enables CTS-SXP on a device.</td>
</tr>
<tr>
<td>cts sxp log</td>
<td>Enables logging for IP-to-SGT binding changes.</td>
</tr>
<tr>
<td>cts sxp reconciliation</td>
<td>Changes the CTS-SXP reconciliation period.</td>
</tr>
<tr>
<td>cts sxp retry</td>
<td>Changes the CTS-SXP retry period timer.</td>
</tr>
<tr>
<td>show cts sxp</td>
<td>Displays the status of all SXP configurations.</td>
</tr>
</tbody>
</table>
**cts sxp default source-ip**

To configure the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) source IPv4 address, use the `cts sxp default source-ip` command in global configuration mode. To remove the CTS-SXP default source IP address, use the `no` form of this command.

```
cts sxp default source-ip ipv4-address
no cts sxp default source-ip ipv4-address
```

**Syntax Description**

| ip-address | Default source CTS-SXP IPv4 address. |

**Command Default**

The CTS-SXP source IP address is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `cts sxp default source-ip` command sets the default source IP address that CTS-SXP uses for all new TCP connections where a source IP address is not specified. Preexisting TCP connections are not affected when this command is entered. CTS-SXP connections are governed by three timers:

- Retry timer
- Delete Hold Down timer
- Reconciliation timer

**Examples**

The following example shows how to enable CTS-SXP and configure the CTS-SXP peer connection on Device_A, a speaker, for connection to Device_B, a listener:

```
Device_A# configure terminal
Device_A(config)# cts sxp enable
Device_A(config)# cts sxp default password Cisco123
Device_A(config)# cts sxp default source-ip 10.10.1.1
Device_A(config)# cts sxp connection peer 10.20.2.2 password default mode local speaker
```

The following example shows how to configure the CTS-SXP peer connection on Device_B, a listener, for connection to Device_A, a speaker:

```
Device_B# configure terminal
Device_B(config)# cts sxp enable
Device_B(config)# cts sxp default password Cisco123
Device_B(config)# cts sxp default source-ip 10.20.2.2
Device_B(config)# cts sxp connection peer 10.10.1.1 password default mode local listener
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts xsp connectionpeer</code></td>
<td>Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.</td>
</tr>
<tr>
<td><code>cts xsp default password</code></td>
<td>Configures the CTS-SXP default password.</td>
</tr>
<tr>
<td><code>cts xsp enable</code></td>
<td>Enables CTS-SXP on a device.</td>
</tr>
<tr>
<td><code>cts xsp log</code></td>
<td>Enables logging for IP-to-SGT binding changes.</td>
</tr>
<tr>
<td><code>cts xsp reconciliation</code></td>
<td>Changes the CTS-SXP reconciliation period.</td>
</tr>
<tr>
<td><code>cts xsp retry</code></td>
<td>Changes the CTS-SXP retry period timer.</td>
</tr>
<tr>
<td><code>show cts xsp</code></td>
<td>Displays the status of all SXP configurations.</td>
</tr>
</tbody>
</table>
cts sxp filter-enable

To enable filtering after creating filter lists and filter groups, use the `cts sxp filter-enable` command in global configuration mode. To disable filtering, use the `no` form of the command.

```
cts sxp filter-enable
no cts sxp filter-enable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be used at any time to enable or disable filtering. Configured filter lists and filter groups can be used to implement filtering only after filtering is enabled. The filter action will only filter bindings that are exchanged after filtering is enabled; there won’t be any effect on the bindings that were exchanged before filtering was enabled.

**Examples**

```
Device(config)# cts sxp filter-enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts sxp filter-list</code></td>
<td>Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both.</td>
</tr>
<tr>
<td><code>cts sxp filter-group</code></td>
<td>Creates a filter group for grouping a set of peers and applying a filter list to them.</td>
</tr>
<tr>
<td><code>show cts sxp filter-group</code></td>
<td>Displays information about the configured filter groups.</td>
</tr>
<tr>
<td><code>show cts sxp filter-list</code></td>
<td>Displays information about the configured filter lists.</td>
</tr>
<tr>
<td><code>debug cts sxp filter events</code></td>
<td>Logs events related to the creation, deletion and update of filter-lists and filter-groups.</td>
</tr>
</tbody>
</table>
**cts sxp filter-group**

To create a filter group for grouping a set of peers and applying a filter list to them, use the `cts sxp filter-group` command in global configuration mode. To delete a filter group, use the `no` form of this command.

```
cts sxp filter-group \{listener | speaker\} \{filter-group-name | global filter-list-name\}
no cts sxp filter-group \{listener | speaker\} \{filter-group-name | global filter-list-name\}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>listener</th>
<th>Creates a filter group for a set of listeners.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>speaker</td>
<td>Creates a filter group for a set of speakers.</td>
</tr>
<tr>
<td></td>
<td>global</td>
<td>Groups all speakers or listeners on the device.</td>
</tr>
<tr>
<td></td>
<td>filter-group-name</td>
<td>Name of the filter group.</td>
</tr>
<tr>
<td></td>
<td>filter-list-name</td>
<td>Name of the filter list.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Issuing this command, places the device in the filter group configuration mode. From this mode, you can specify the devices to be grouped and apply a filter list to the filter group.

The command format to add devices or peers to the group is as follows:

```
peer ipv4 peer-IP
```

In a single command, you can add one peer. To add more peers, repeat the command as many times as required.

The command format to apply a filter list to the group is as follows:

```
filter filter-list-name
```

You cannot specify a peer list for the global listener and global speaker filter-group options because in this case the filter is applied to all SXP connections.

When both the global filter group and peer-based filter groups are applied, the global filter takes priority. If only a global listener or global speaker filter group is configured, then the global filtering takes precedence only in that specific direction. For the other direction, the peer-based filter group is implemented.

**Examples**

The following example shows how to create a listener group called `group_1`, and assign peers and a filter list to this group:

```
Device# configure terminal
Device(config)# cts sxp filter-group listener group_1
Device(config-filter-group)# filter filter_1
```
Device(config-filter-group)# peer ipv4 10.0.0.1
Device(config-filter-group)# peer ipv4 10.10.10.1

The following example shows how to create a global listener group called `group_2`:

Device# configure terminal
Device(config)# cts sxp filter-group listener global group_2

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts sxp filter-list</td>
<td>Creates a SXP filter list to filter IP-SGT bindings based on IP prefixes, SGT or a combination of both.</td>
</tr>
<tr>
<td>cts sxp filter-enable</td>
<td>Enables filtering.</td>
</tr>
<tr>
<td>show cts sxp filter-group</td>
<td>Displays information about the configured filter groups.</td>
</tr>
<tr>
<td>show cts sxp filter-list</td>
<td>Displays information about the configured filter lists.</td>
</tr>
<tr>
<td>debug cts sxp filter events</td>
<td>Logs events related to the creation, deletion and update of filter-lists and filter-groups</td>
</tr>
</tbody>
</table>
**cts sxp filter-list**

To create a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings, use the `cts sxp filter-list` command in global configuration mode. To delete a filter list, use the `no` form of the command.

```
cts sxp filter-list  filter-list-name
no cts sxp filter-list  filter-list-name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filter-list-name</code></td>
<td>Name of the filter-list.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Fuji 16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Issuing this command, places the device in the filter list configuration mode. From this mode, you can specify rules for the filter lists.

A filter rule can be based on SGT or IP Prefixes or a combination of both SGT and IP Prefixes.

The command format to add rules to the group is as follows:

```
sequence-number  action(permit/deny)  filter-type(ipv4/ipv6/sgt)  value/values
```

For example, to permit SGT-IP bindings whose SGT value is 20, the rule is as follows:

```
30 permit sgt 20
```

Note that the sequence number is optional. If you do not specify a sequence number, it is generated by the system. Sequence numbers are automatically incremented by a value of 10 from the last used/configured sequence number. A new rule can be inserted by specifying a sequence number in between two existing rules.

The range of valid SGT values is between 2 and 65519. To provide multiple SGT values in a rule, separate the values using a space. A maximum of 8 SGT values are allowed in a rule.

In a SGT and IP prefix combination rule, if there is a match for the binding in both the parts of the rule, then the action specified in the second part of the rule takes precedence. For example, in the following rule, if the SGT value of the IP prefix 10.0.0.1 is 20, the corresponding binding will be denied even if the first part of the rule permits the binding.

```
Device(config-filter-list)# 10 permit sgt 30 20 deny 10.0.0.1/24
```

Similarly, in the rule below the binding with the sgt value 20 will be permitted even if the sgt of the IP prefix 10.0.0.1 is 20, and the first action does not permit the binding.

```
Device(config-filter-list)# 10 deny 10.0.0.1/24 permit sgt 30 20
```

**Examples**

The following example shows how to create a filter list and add some rules to the list:
Device# configure terminal
Device(config)# cts sxp filter-list filter_1
Device (config-filter-list)# 10 deny ipv4 10.0.0.1/24 permit sgt 100
Device(config-filter-list)# 20 permit sgt 60 61 62 63

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cts sxp filter-enable</td>
<td>Enable SXP IP-prefix and SGT-based filtering.</td>
</tr>
<tr>
<td></td>
<td>cts sxp filter-group</td>
<td>Creates a filter group for grouping a set of peers and applying a filter list to them.</td>
</tr>
<tr>
<td></td>
<td>show cts sxp filter-group</td>
<td>Displays information about the configured filter groups.</td>
</tr>
<tr>
<td></td>
<td>show cts sxp filter-list</td>
<td>Displays information about the configured filter lists.</td>
</tr>
<tr>
<td></td>
<td>debug cts sxp filter events</td>
<td>Logs events related to the creation, deletion and update of filter-lists and filter-groups.</td>
</tr>
</tbody>
</table>
To enable logging for IP-to-Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) binding changes, use the `cts sxp log binding-changes` command in global configuration mode. To disable logging, use the `no` form of this command.

```
cts sxp log binding-changes
no cts sxp log binding-changes
```

**Command Default**

Logging is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `cts sxp log binding-changes` command enables logging for IP-to-SGT binding changes. SXP syslogs (seq 5 syslogs) are generated whenever IP address-to-SGT binding occurs (add, delete, change). These changes are learned and propagated on the SXP connection.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts sxp connectionpeer</code></td>
<td>Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection</td>
</tr>
<tr>
<td><code>cts sxp default password</code></td>
<td>Configures the CTS-SXP default password.</td>
</tr>
<tr>
<td><code>cts sxp default source-ip</code></td>
<td>Configures the CTS-SXP source IPv4 address.</td>
</tr>
<tr>
<td><code>cts sxp enable</code></td>
<td>Enables CTS-SXP on a device.</td>
</tr>
<tr>
<td><code>cts sxp reconciliation</code></td>
<td>Changes the CTS-SXP reconciliation period.</td>
</tr>
<tr>
<td><code>cts sxp retry</code></td>
<td>Changes the CTS-SXP retry period timer.</td>
</tr>
<tr>
<td><code>show cts sxp</code></td>
<td>Displays status of all SXP configurations.</td>
</tr>
</tbody>
</table>
cts xsp reconciliation period

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) reconciliation period, use the `cts xsp reconciliation period` command in global configuration mode. To return the CTS-SXP reconciliation period to its default value, use the `no` form of this command.

```
cts xsp reconciliation period seconds
no cts xsp reconciliation period seconds
```

**Syntax Description**

| `seconds` | CTS-SXP reconciliation timer in seconds. The range is from 0 to 64000. The default is 120. |

**Command Default**

120 seconds (2 minutes)

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After a peer terminates a CTS-SXP connection, an internal delete hold-down timer starts. If the peer reconnects before the delete hold-down timer expires, then the CTS-SXP reconciliation timer starts. While the CTS-SXP reconciliation period timer is active, the CTS-SXP software retains the SGT mapping entries learned from the previous connection and removes invalid entries. Setting the SXP reconciliation period to 0 seconds disables the timer and causes all entries from the previous connection to be removed.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts xsp connection peer</code></td>
<td>Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.</td>
</tr>
<tr>
<td><code>cts xsp default password</code></td>
<td>Configures the CTS-SXP default password.</td>
</tr>
<tr>
<td><code>cts xsp default source-ip</code></td>
<td>Configures the CTS-SXP source IPv4 address.</td>
</tr>
<tr>
<td><code>cts xsp enable</code></td>
<td>Enables CTS-SXP on a device.</td>
</tr>
<tr>
<td><code>cts xsp log</code></td>
<td>Turns on logging for IP to SGT binding changes.</td>
</tr>
<tr>
<td><code>cts xsp retry</code></td>
<td>Changes the CTS-SXP retry period timer.</td>
</tr>
<tr>
<td><code>show cts xsp</code></td>
<td>Displays status of all CTS-SXP configurations.</td>
</tr>
</tbody>
</table>
**cts sxp retry period**

To change the Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) retry period timer, use the `cts sxp retry period` command in global configuration mode. To return the CTS-SXP retry period timer to its default value, use the `no` form of this command.

```
cts sxpretry period seconds
no cts sxpretry period seconds
```

**Syntax Description**

`seconds` | CTS-SXP retry timer in seconds. The range is from 0 to 64000. The default is 120.

**Command Default**

120 seconds (2 minutes)

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The retry timer is triggered if there is at least one CTS-SXP connection that is not up. A new CTS-SXP connection is attempted when this timer expires. A zero value results in no retry being attempted.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cts sxp connectionpeer</code></td>
<td>Enters the CTS-SXP peer IP address and specifies if a password is used for the peer connection.</td>
</tr>
<tr>
<td><code>cts sxp default password</code></td>
<td>Configures the CTS-SXP default password.</td>
</tr>
<tr>
<td><code>cts sxp default source-ip</code></td>
<td>Configures the CTS-SXP source IPv4 address.</td>
</tr>
<tr>
<td><code>cts sxp enable</code></td>
<td>Enables CTS-SXP on a device.</td>
</tr>
<tr>
<td><code>cts sxp log</code></td>
<td>Enables logging for IP-to-SGT binding changes.</td>
</tr>
<tr>
<td><code>cts sxp reconciliation</code></td>
<td>Changes the CTS-SXP reconciliation period.</td>
</tr>
<tr>
<td><code>show cts sxp</code></td>
<td>Displays the status of all CTS-SXP configurations.</td>
</tr>
</tbody>
</table>
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.

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

### 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:

```
Device# configure terminal
Device(config)# interface gigabitethernet 0
Device(config-if)# cts manual
Device(config-if-cts-manual)# no propagate sgt
```

The following example shows that SGT propagation is disabled on Gigabit Ethernet interface 0:

```
Device# 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts manual</td>
<td>Enables an interface for CTS.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>show cts interface</td>
<td>Displays Cisco TrustSec states and statistics per interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>pmk hex_value</th>
<th>Specifies the Hex-data PMK (without leading 0x; enter even number of hex characters, or else the last character is prefixed with 0.).</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode-list</td>
<td>Specifies the list of advertised modes (prioritized from highest to lowest).</td>
</tr>
<tr>
<td>gcm-encrypt</td>
<td>Specifies GMAC authentication, GCM encryption.</td>
</tr>
<tr>
<td>gmac</td>
<td>Specifies GMAC authentication only, no encryption.</td>
</tr>
<tr>
<td>no-encap</td>
<td>Specifies no encapsulation.</td>
</tr>
<tr>
<td>null</td>
<td>Specifies encapsulation present, no authentication, no encryption.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device# configure terminal
Device(config)# interface gigabitethernet 2/1
Device(config-if)# cts manual
Device(config-if-cts-manual)# sap pmk FFFEE mode-list gcm-encrypt
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>cts manual</td>
<td>Enables an interface for CTS.</td>
</tr>
<tr>
<td></td>
<td>show cts interface</td>
<td>Displays Cisco TrustSec interface configuration statistics.</td>
</tr>
</tbody>
</table>
show cts credentials

To display the Cisco TrustSec (CTS) device ID, use the `show cts credentials` command in EXEC or privileged EXEC mode.

`show cts credentials`

**Syntax Description**

This command has no commands or keywords.

**Command Modes**

Privileged EXEC (###)  User EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fiji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays output:

```
Device# show cts credentials
CTS password is defined in keystore, device-id = r4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts credentials</td>
<td>Specifies the TrustSec ID and password.</td>
</tr>
</tbody>
</table>
show cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface(s), use the `show cts interface` command in EXEC or privileged EXEC mode.

```
show cts interface [{GigabitEthernet port | Vlan number | brief | summary}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>port</code></td>
<td>(Optional) Gigabit Ethernet interface number. A verbose status output for this interface is returned.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>(Optional) VLAN interface number from 1 to 4095.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>(Optional) Displays abbreviated status for all CTS interfaces.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC (>)
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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):

```
Device# 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:
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts manual</td>
<td>Enables an interface for CTS.</td>
</tr>
<tr>
<td>cts sxp enable</td>
<td>Configures SXP on a network device.</td>
</tr>
<tr>
<td>propagate sgt</td>
<td>Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.</td>
</tr>
</tbody>
</table>
show cts role-based counters

To display Security Group access control list (ACL) enforcement statistics, use the show cts role-based counters command in user EXEC or privileged EXEC mode.

show cts role-based counters <![CDATA[default [ipv4 | ipv6]]] [from [sgt-number | unknown] [ipv4 | ipv6] to [sgt-number | unknown]] [to [sgt-number | unknown] [ipv4 | ipv6]] [ipv4 | ipv6]]

Syntax Description

default
(Optional) Displays information about the default policy counters.

from
(Optional) Displays information about the source security group.

ipv4
(Optional) Displays information about security groups on IPv4 networks.

ipv6
(Optional) Displays information about security groups on IPv6 networks.

to
(Optional) Displays information about the destination security group.

sgt-number
(Optional) Security Group Tag number. Valid values are from 0 to 65533.

unknown
(Optional) Displays information about all source groups.

Command Modes

User EXEC (>

Privileged EXEC (#)

Command History

Release Modification
Cisco IOS XE Fuji 16.9.1 This command was introduced.

Usage Guidelines

Use the clear cts role-based counters command to reset all or a range of statistics.

Specify the source SGT with the from keyword and the destination SGT with the to keyword. All statistics are displayed when both the from and to keywords are omitted.

The default keyword displays the statistics of the default unicast policy. When neither ipv4 nor ipv6 keywords are specified, this command displays only IPv4 counters.

In Cisco TrustSec monitor mode, permitted traffic counters are displayed under the SW-Permitt label and the denied traffic counters are displayed under SW-Monitor label.
Example

The following is sample output from the `show cts role-based counters`

```
Device# show cts role-based counters

Role-based IPv4 counters
From To SW-Denied HW-Denied SW-Permitt HW-Permitt SW-Monitor HW-Monitor
12 24 0 0 0 0 0 0
12 77 0 0 5 0 0 0
```

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

**Table 6: show cts role-based counters Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From</td>
<td>Source security group.</td>
</tr>
<tr>
<td>To</td>
<td>Destination security group.</td>
</tr>
<tr>
<td>SW-Permit</td>
<td>Permitted traffic counters.</td>
</tr>
<tr>
<td>SW-Monitor</td>
<td>Denied traffic counters.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear role-basedcounters</td>
<td>Resets SGACL statistic counters.</td>
</tr>
<tr>
<td>cts role-based</td>
<td>Maps IP addresses, Layer 3 interfaces, and VRFs to SGTs. Enables Cisco TrustSec caching and SGACL enforcement.</td>
</tr>
</tbody>
</table>
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] | ipv6 [details]}]} | from { {sgt | unknown} [{ipv4 | ipv6} | to {sgt | unknown} [{details | ipv4 [details] | ipv6 [details]}]}]} | ipv4 | ipv6 | platform | to {sgt | unknown} [{ipv4 | ipv6}]
```

**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.
- `ipv6` (Optional) Displays information about the IPv6 protocol.
- `from` (Optional) Displays information about the source group.
- `sgt` (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.
- `platform` (Optional) Displays information about the platform.

**Command Modes**

Privileged EXE (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device# 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts role-based permissions</td>
<td>Enables permissions from a source group to a destination group.</td>
</tr>
<tr>
<td>cts role-based monitor</td>
<td>Enables role-based access list monitoring.</td>
</tr>
</tbody>
</table>
show cts server-list

To display the list of RADIUS servers available to Cisco TrustSec (CTS) seed and nonseed devices, use the `show cts server-list` command in user EXEC or privileged EXEC mode.

**Syntax Description**

This command has no commands or keywords.

**Command Modes**

Privileged EXEC (#) User EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is useful for gathering CTS RADIUS server address and status information.

**Examples**

The following example displays the CTS RADIUS server list:

```
Device> show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
  *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
    Status = ALIVE
    auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
  *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
    Status = ALIVE
    auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address ipv4 (config-radius-server)</td>
<td>Configures the RADIUS server accounting and authentication parameters for PAC provisioning.</td>
</tr>
<tr>
<td>pac key</td>
<td>Specifies the PAC encryption key.</td>
</tr>
</tbody>
</table>
show cts sxp

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the `show cts sxp` command in user EXEC or privileged EXEC mode.

```
show cts sxp {connections [{brief | vrf instance-name}] | filter-group [{detailed | global | listener | speaker}] | filter-list filter-list-name | sgt-map [{brief | vrf instance-name}]} [{brief | vrf instance-name}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connections</td>
<td>Displays Cisco TrustSec SXP connections information.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays an abbreviation of the SXP information.</td>
</tr>
<tr>
<td>vrf instance-name</td>
<td>(Optional) Displays the SXP information for the specified VRF instance name.</td>
</tr>
<tr>
<td>filter-group</td>
<td>(Optional) Displays filter group information.</td>
</tr>
<tr>
<td>listener</td>
<td>speaker</td>
</tr>
<tr>
<td>filter-list filter-list-name</td>
<td>(Optional) Displays the IP-to-SGT mappings received through SXP.</td>
</tr>
<tr>
<td>sgt-map</td>
<td>(Optional) Displays the IP-to-SGT mappings received through SXP.</td>
</tr>
</tbody>
</table>

### Command Default
None

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

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example displays the SXP connections using the `brief` keyword:

```
Device# show cts sxp connection brief

SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
-----------------------------------------------------------------------------
Peer_IP Source_IP Conn Status Duration                
-----------------------------------------------------------------------------
10.10.10.1 10.10.10.2 On 0:00:02:14 (dd:hr:mm:sec) 
10.10.2.1 10.10.2.2 On 0:00:02:14 (dd:hr:mm:sec) 
Total num of SXP Connections = 2
```
The following example displays the CTS-SXP connections:

Device# show cts sxp connections

SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running

Peer IP : 10.10.10.1
Source IP : 10.10.10.2
Set up : Peer
Conn status : On
Connection mode : SXP Listener
Connection inst# : 1
TCP conn fd : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)

Peer IP : 10.10.2.1
Source IP : 10.10.2.2
Set up : Peer
Conn status : On
Connection mode : SXP Listener
TCP conn fd : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)

Total num of SXP Connections = 2

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running

Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the delete hold down timer.

Device# show cts sxp connections

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running

----------------------------------------------
Peer IP : 10.10.10.1
Source IP : 10.10.10.2
Set up : Peer
Conn status : Delete_Hold_Down
Connection mode : SXP Listener
Connection inst# : 1
TCP conn fd : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)

----------------------------------------------
Peer IP : 10.10.2.1
Source IP : 10.10.2.2
Set up : Peer
Conn status : On
Connection inst# : 1
TCP conn fd : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cts xsp connection peer</td>
<td>Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection</td>
</tr>
<tr>
<td>cts xsp default password</td>
<td>Configures the Cisco TrustSec SXP default password.</td>
</tr>
<tr>
<td>cts xsp default source-ip</td>
<td>Configures the Cisco TrustSec SXP source IPv4 address.</td>
</tr>
<tr>
<td>cts xsp enable</td>
<td>Enables Cisco TrustSec SXP on a device.</td>
</tr>
<tr>
<td>cts xsp log</td>
<td>Enables logging for IP-to-SGT binding changes.</td>
</tr>
<tr>
<td>cts xsp reconciliation</td>
<td>Changes the Cisco TrustSec SXP reconciliation period.</td>
</tr>
<tr>
<td>cts xsp retry</td>
<td>Changes the Cisco TrustSec SXP retry period timer.</td>
</tr>
</tbody>
</table>
show cts sxp
PART II

High Availability

- High Availability Commands, on page 65
High Availability Commands

- clear diagnostic event-log, on page 67
- diagnostic monitor, on page 68
- diagnostic schedule module, on page 70
- diagnostic start, on page 73
- diagnostic stop, on page 76
- domain id, on page 78
- dual-active detection pagp, on page 79
- dual-active recovery-reload-disable, on page 80
- hw-module beacon switch, on page 81
- hw-module switch slot, on page 82
- hw-module switch ushflash, on page 84
- main-cpu, on page 85
- maintenance-template, on page 86
- mode sso, on page 87
- policy config-sync prc reload, on page 88
- redundancy, on page 89
- reload, on page 90
- router routing protocol shutdown l2, on page 92
- set platform software fed switch, on page 93
- set platform software nif-mgr switch, on page 94
- show diagnostic bootup, on page 95
- show diagnostic content, on page 96
- show diagnostic description, on page 100
- show diagnostic events, on page 102
- show diagnostic result, on page 104
- show diagnostic simulation failure, on page 109
- show diagnostic schedule, on page 110
- show hw-module switch subslot, on page 111
- show logging onboard switch, on page 113
- show platform software fed , on page 116
- show platform software nif-mgr switch , on page 119
- show redundancy, on page 123
- show redundancy config-sync, on page 127
- show stackwise-virtual, on page 129
- show tech-support stack, on page 131
- stackwise-virtual, on page 136
- stackwise-virtual dual-active-detection, on page 137
- stackwise-virtual link, on page 138
- standby console enable, on page 139
- start maintenance, on page 140
- stop maintenance, on page 141
- system mode maintenance, on page 142
clear diagnostic event-log

To clear the diagnostic event logs for a specific switch module or event type, use the `clear diagnostic event-log` command in privileged EXEC mode.

```
clear diagnostic event-log [{event-type {error | info | warning}} | switch {switch_num | module module_num | all [{event-type {error | info | warning}}]}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>event-type error</code></td>
<td>Clears the error events.</td>
</tr>
<tr>
<td><code>event-type info</code></td>
<td>Clears the informative events.</td>
</tr>
<tr>
<td><code>event-type warning</code></td>
<td>Clears the warning events.</td>
</tr>
<tr>
<td><code>switch num</code></td>
<td>Clears the events for a specific switch.</td>
</tr>
<tr>
<td><code>module num</code></td>
<td>Clears the events for a specific module.</td>
</tr>
<tr>
<td><code>switch all</code></td>
<td>Clears all the event logs from all the switches.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear error event logs:

```
Device# clear diagnostic event-log event-type error
```

This example shows how to clear event logs on switch 1 module 1:

```
Device# clear diagnostic event-log switch 1 module 1
```

This example shows how to clear error event logs on all the switches:

```
Device# clear diagnostic event-log switch all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diagnostic events</code></td>
<td>Displays the diagnostic event log.</td>
</tr>
</tbody>
</table>
To configure health-monitoring diagnostic testing, use the **diagnostic monitor** command in global configuration mode. Use the **no** form of this command to disable testing and to return to the default settings.

```plaintext
diagnostic monitor interval switch number module number test {name | test-id | test-id-range | all} hh:mm:ss milliseconds day [cardindex number]
diagnostic monitor switch number module number test {name | test-id | test-id-range | all} [cardindex number]
diagnostic monitor threshold switch number module number test {name | test-id | test-id-range | all} failure count count [days number | hours number | milliseconds number | minutes number | runs number | seconds number] cardindex number
no diagnostic monitor interval switch number module number test {name | test-id | test-id-range | all} [cardindex number]
no diagnostic monitor switch number module number test {name | test-id | test-id-range | all} [cardindex number]
no diagnostic monitor threshold switch number module number test {name | test-id | test-id-range | all} failure count count [days number | hours number | milliseconds number | minutes number | runs number | seconds number] cardindex number [cardindex number]
```

### Syntax Description

<table>
<thead>
<tr>
<th><strong>interval</strong></th>
<th>Configures the interval between tests.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>switch number</strong></td>
<td>Specifies the switch number, which is the stack member number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is from 1 to 9, depending on the switch member numbers in the stack. This keyword is supported only on on stacking-capable switches.</td>
</tr>
<tr>
<td><strong>test</strong></td>
<td>Specifies the tests to be run.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>Name of the test.</td>
</tr>
<tr>
<td><strong>test-id</strong></td>
<td>ID number of the test.</td>
</tr>
<tr>
<td><strong>test-id-range</strong></td>
<td>Range of test ID numbers. Enter the range as integers separated by a comma and a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>Specifies all the diagnostic tests.</td>
</tr>
<tr>
<td><strong>hh:mm:ss</strong></td>
<td>Monitoring interval, in hours, minutes, and seconds. Enter the hours from 0 to 24, minutes from 0 to 60, and seconds from 0 to 60.</td>
</tr>
</tbody>
</table>
### Command Default
Monitoring is disabled, and a failure threshold value is not set.

### Command Modes
Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
You must configure the failure threshold and the interval between tests before enabling diagnostic monitoring.

When entering the `diagnostic monitor switch module test` command, you must isolate network traffic by disabling all the connected ports, and not send test packets during a test.

### Examples
This example shows how to set the failure threshold count of Test 1 to 20:

```
Device# configure terminal
Device(config)# diagnostic monitor threshold switch 2 test 1 failure count 20
```

This example shows how to configure the monitoring interval of Test 2:

```
Device# configure terminal
Device(config)# diagnostic monitor interval switch 2 test 2 12:30:00 750 5
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show diagnostic content switch module</code></td>
<td>Displays online diagnostic test results.</td>
</tr>
</tbody>
</table>
diagnostic schedule module

To schedule test-based diagnostic task for a specific switch module or schedule a supervisor engine switchover, use the `diagnostic schedule switch module` command in global configuration mode. To remove the schedule, use the `no` form of this command.

```
diagnostic schedule switch number module module-num test {test-id | {complete | minimal} {daily hh:mm | on month | weekly day-of-week} | {all | basic | non-disruptive | per-port} {daily hh:mm | on month | weekly day-of-week}} | weekly day-of-week}}
```

```
no diagnostic schedule switch number module module-num test {test-id | {complete | minimal} {daily hh:mm | on month | weekly day-of-week} | {all | basic | non-disruptive | per-port} {daily hh:mm | on month | weekly day-of-week}} | weekly day-of-week}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch_num</td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td>module module_num</td>
<td>Specifies the module number.</td>
</tr>
<tr>
<td>test</td>
<td>Specifies the diagnostic test suite attribute.</td>
</tr>
<tr>
<td>test-id</td>
<td>Identification number for the test to be run.</td>
</tr>
<tr>
<td></td>
<td>Enter the <code>show diagnostic content</code> command to display the test ID list.</td>
</tr>
<tr>
<td>all</td>
<td>Runs all the diagnostic tests.</td>
</tr>
<tr>
<td>complete</td>
<td>Selects the complete bootup test suite.</td>
</tr>
<tr>
<td>minimal</td>
<td>Selects the minimal bootup test suite.</td>
</tr>
<tr>
<td>non-disruptive</td>
<td>Selects the nondisruptive test suite.</td>
</tr>
<tr>
<td>per-port</td>
<td>Selects the per-port test suite.</td>
</tr>
<tr>
<td></td>
<td><code>per-port</code> is not supported when specifying a scheduled switchover.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Specifies the port-to-schedule testing.</td>
</tr>
<tr>
<td>interface-port-number</td>
<td>(Optional) Port number. The range is from 1-48.</td>
</tr>
<tr>
<td>port-number-list</td>
<td>(Optional) Range of port numbers, separated by a hyphen. The range is from 1-48.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Specifies all the ports.</td>
</tr>
<tr>
<td>on month</td>
<td>Specifies the schedule of a test-based diagnostic task.</td>
</tr>
<tr>
<td></td>
<td>Enter the month name, for example, January or February (either uppercase or lowercase characters).</td>
</tr>
</tbody>
</table>

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Specifies the daily schedule of a test-based diagnostic task.
Enter the time as a two-digit number (for a 24-hour clock) for hours:minutes; the colon (:) is required.

Specifies the weekly schedule of a test-based diagnostic task.
Enter the day of the week, for example, Monday or Tuesday (either uppercase or lowercase characters).

Test-based diagnostic task for a specific switch module is not scheduled.

Global configuration (config)

Cisco IOS XE Fiji 16.9.1 This command was introduced.

Run the `diagnostic schedule switch module test` command to schedule a switchover from the active supervisor engine to the standby supervisor engine.
The `show diagnostic content switch module` command displays the test ID list. The test ID is displayed in the `ScheduleSwitchover` field.
You can specify a periodic switchover (daily or weekly) or a single switchover occurrence at a specific time using these commands:

- `diagnostic schedule switch number module module_num test test-id on mm`
- `diagnostic schedule switch number module module_num test test-id daily hh:mm`
- `diagnostic schedule switch number module module_num test test-id weekly day-of-week`

To avoid system downtime in the event that the standby supervisor module cannot switch over the system, we recommend that you schedule a switchover from the standby supervisor module to the active supervisor module 10 minutes after the switchover occurs.

This example shows how to schedule diagnostic testing on a specific month, date, and time for a specific switch module:

```
Device# configure terminal
Device(config)# diagnostic schedule switch 1 module 1 test 5 on may
```

This example shows how to schedule diagnostic testing to occur daily at a certain time for a specific switch module:

```
Device# configure terminal
Device(config)# diagnostic schedule switch 1 module 1 test 5 daily 12:25
```

This example shows how to schedule diagnostic testing to occur weekly on a certain day for a specific switch module:

```
Device# configure terminal
Device(config)# diagnostic schedule switch 1 module 1 test 5 weekly Monday
```
Device# configure terminal
Device(config)# diagnostic schedule module 1 test 5 weekly friday

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show diagnostic content</td>
<td>Displays test information, including test ID, test attributes, and supported coverage test levels for all the tests and modules.</td>
</tr>
<tr>
<td></td>
<td>show diagnostic schedule</td>
<td>Displays the current scheduled diagnostic tasks.</td>
</tr>
</tbody>
</table>
diagnostic start

To run a specified diagnostic test, use the diagnostic start command in privileged EXEC mode.

diagnostic start switch number module module_num test {test-id | minimal | complete | {{all | basic | non-disruptive | per-port | port {num | port_range | all}}}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch_num</td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td>module module_num</td>
<td>Specifies the module number.</td>
</tr>
<tr>
<td>test</td>
<td>Specifies a test to run.</td>
</tr>
<tr>
<td>test-id</td>
<td>Enter the identification number of the test you want to run.</td>
</tr>
<tr>
<td></td>
<td>Enter the test-id-range or port_range as integers separated by a comma and</td>
</tr>
<tr>
<td></td>
<td>a hyphen (for example, 1,3-6 specifies test IDs 1, 3, 4, 5, and 6).</td>
</tr>
<tr>
<td>minimal</td>
<td>Runs minimal bootup diagnostic tests.</td>
</tr>
<tr>
<td>complete</td>
<td>Runs complete bootup diagnostic tests.</td>
</tr>
<tr>
<td>basic</td>
<td>Runs basic on-demand diagnostic tests.</td>
</tr>
<tr>
<td>per-port</td>
<td>Runs per-port level tests.</td>
</tr>
<tr>
<td>non-disruptive</td>
<td>Runs nondisruptive health-monitoring tests.</td>
</tr>
<tr>
<td>all</td>
<td>Runs all the diagnostic tests.</td>
</tr>
<tr>
<td>port num</td>
<td>(Optional) Specifies the interface port number. The range is from 1-48.</td>
</tr>
</tbody>
</table>

Command Default
None

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Run the show diagnostic content command to display the test ID list.
Use the diagnostic stop command to stop the testing process.

Examples

This example shows how to run the complete online diagnostic tests:

Device# diagnostic start switch 1 module 1 test all

Diagnostic[switch 1, module 1]: Running test(s) 2 may disrupt normal system operation and requires reload
Do you want to continue? [no]: y

Device#*

Jul 5 03:04:49.081 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestGoldPktLoopback[ID=1] ...
Jul 5 03:04:49.086 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestGoldPktLoopback[ID=1] has completed successfully
Jul 5 03:04:49.086 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestPhyLoopback[ID=2] ...
Jul 5 03:04:49.092 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPhyLoopback[ID=2] has completed successfully
Jul 5 03:04:49.092 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running TestThermal[ID=3] ...
Jul 5 03:04:52.397 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestThermal[ID=3] has completed successfully
Jul 5 03:04:52.397 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestScratchRegister[ID=4] ...
Jul 5 03:04:52.414 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestScratchRegister[ID=4] has completed successfully
Jul 5 03:04:52.414 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running TestPoe[ID=5] ...
Jul 5 03:04:52.415 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPoe[ID=5] has completed successfully
Jul 5 03:04:52.415 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running
TestUnusedPortLoopback[ID=6] ...
Jul 5 03:04:52.415 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestUnusedPortLoopback[ID=6] has completed successfully
Jul 5 03:04:52.415 PDT: %DIAG-6-TEST_RUNNING: switch 1, module 1: Running TestPortTxMonitoring[ID=7] ...
Jul 5 03:04:52.416 PDT: %DIAG-6-TEST_OK: switch 1, module 1: TestPortTxMonitoring[ID=7] has completed successfully

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic bootup level</td>
<td>Configures the diagnostic bootup level.</td>
</tr>
<tr>
<td>diagnostic event-log size</td>
<td>Modifies the diagnostic event log size dynamically.</td>
</tr>
<tr>
<td>diagnostic monitor</td>
<td>Configures health-monitoring diagnostic testing.</td>
</tr>
<tr>
<td>diagnostic ondemand</td>
<td>Configures the on-demand diagnostics.</td>
</tr>
<tr>
<td>diagnostic schedule</td>
<td>Sets the diagnostic test schedule for a particular bay, slot, or subslot.</td>
</tr>
<tr>
<td>diagnostic stop</td>
<td>Stops a specified diagnostic test.</td>
</tr>
<tr>
<td>show diagnostic bootup</td>
<td>Displays the configured diagnostics level at bootup.</td>
</tr>
<tr>
<td>show diagnostic content module</td>
<td>Displays the available diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic description</td>
<td>Provides the description for diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic events</td>
<td>Displays the diagnostic event log.</td>
</tr>
<tr>
<td>show diagnostic ondemand settings</td>
<td>Displays the settings for the on-demand diagnostics.</td>
</tr>
<tr>
<td>show diagnostic result</td>
<td>Displays the diagnostic test results for a module.</td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Displays the current scheduled diagnostic tasks.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the running diagnostics tests.</td>
</tr>
</tbody>
</table>
To stop the testing process, use the diagnostic stop command in privileged EXEC mode.

```
diagnostic stop switch number module module_num
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch_num</td>
<td>Specifies the switch number.</td>
</tr>
<tr>
<td>module module_num</td>
<td>Specifies the module number.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the diagnostic start command to start the testing process.

**Examples**

This example shows how to stop the diagnostic test process:

```
Device# diagnostic stop module 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diagnostic bootup level</td>
<td>Configures the diagnostic bootup level.</td>
</tr>
<tr>
<td>diagnostic event-log size</td>
<td>Modifies the diagnostic event log size dynamically.</td>
</tr>
<tr>
<td>diagnostic monitor</td>
<td>Configures health-monitoring diagnostic testing.</td>
</tr>
<tr>
<td>diagnostic ondemand</td>
<td>Configures the on-demand diagnostics.</td>
</tr>
<tr>
<td>diagnostic schedule</td>
<td>Sets the diagnostic test schedule for a particular bay, slot, or subslot.</td>
</tr>
<tr>
<td>diagnostic start</td>
<td>Runs a specified diagnostic test.</td>
</tr>
<tr>
<td>show diagnostic bootup</td>
<td>Displays the configured diagnostics level at bootup.</td>
</tr>
<tr>
<td>show diagnostic content module</td>
<td>Displays the available diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic description</td>
<td>Provides the description for the diagnostic tests.</td>
</tr>
<tr>
<td>show diagnostic events</td>
<td>Displays the diagnostic event log.</td>
</tr>
<tr>
<td>show diagnostic ondemand settings</td>
<td>Displays the settings for the on-demand diagnostics.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show diagnostic result</td>
<td>Displays the diagnostic test results for a module.</td>
</tr>
<tr>
<td>show diagnostic schedule</td>
<td>Displays the current scheduled diagnostic tasks.</td>
</tr>
<tr>
<td>show diagnostic status</td>
<td>Displays the running diagnostics tests.</td>
</tr>
</tbody>
</table>
To configure Cisco StackWise Virtual domain ID on a switch, use the `domain id` command in the StackWise Virtual configuration mode. To disable, use the `no` form of this command.

```plaintext
domain id
no domain id
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>domain</code></td>
<td>Associates StackWise Virtual configuration with a specific domain.</td>
</tr>
<tr>
<td><code>id</code></td>
<td>Value of the domain ID. The range is from 1 to 255. The default is one.</td>
</tr>
</tbody>
</table>

### Command Default

No domain ID is configured.

### Command Modes

StackWise Virtual configuration (config-stackwise-virtual)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command is optional. You must enable Stackwise Virtual, using the `stackwise-virtual` command, before configuring the domain ID.

### Example

The following example shows how to enable Cisco StackWise Virtual and configure a domain ID:

```plaintext
Device(config)# stackwise-virtual
Device(config-stackwise-virtual)#domain 2
```
**dual-active detection pagp**

To enable PAgP dual-active detection, use the `dual-active detection pagp` command in the StackWise Virtual configuration mode. To disable PAgP dual-active detection, use the `no` form of the command.

```
dual-active detection pagp
no dual-active detection pagp
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dual-active detection pagp</code></td>
<td>Enables pAgp dual-active detection.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled.

**Command Modes**

StackWise Virtual configuration (config-stackwise-virtual)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to enable PAgP dual-active detection trust mode on channel-group:

```
Device(config)# stackwise-virtual
Device(config-stackwise-virtual)# dual-active detection pagp
Device(config-stackwise-virtual)# dual-active detection pagp trust channel-group 1
```
dual-active recovery-reload-disable

To disable automatic recovery reload of a switch, use the `dual-active recovery-reload-disable` command in the StackWise Virtual configuration mode. To enable automatic recovery reload, use the `no` form of the command.

```
dual-active recovery-reload-disable
no dual-active recovery-reload-disable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dual-active recovery-reload-disable</td>
<td>Disables automatic recovery reload.</td>
</tr>
</tbody>
</table>

**Command Default**

Enabled.

**Command Modes**

StackWise Virtual configuration (config-stackwise-virtual)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to disable automatic recovery reload of a switch:

```
Device(config)# stackwise-virtual
Device(config-stackwise-virtual)# dual-active recovery-reload-disable
```
To control the blue beacon LED in a field-replaceable unit (FRU), use the `hw-module beacon switch` command in privileged EXEC mode.

```
hw-module beacon switch { switch-number | active | standby } { RP { active | standby } | fan-tray | power-supply power-supply slot number | slot slot number } { off | on | status }
```

**Syntax Description**

- **switch-number**
  The switch to access. Valid values are 1 and 2.

- **active**
  Selects the active instance of the switch.

- **standby**
  Selects the standby instance of the switch.

- **RP**
  Selects the route processor for the selected switch.

- **fan-tray**
  Selects the fan for the selected switch.

- **power-supply**
  Selects the power supply slot number. Valid values are 1 to 4.

- **power-supply slot number**
  Specifies the power supply slot number. Valid values are 1 to 4.

- **slot slot-number**
  Specifies the slot number. Valid values are 1 to 4.

- **off**
  Switches off the beacon LED for the route processor and the slot, and switches off the fan and the power supply for the selected switch.

- **on**
  Switches on the beacon LED for the route processor and the slot, and switches off the fan and the power supply for the selected switch.

- **status**
  Displays the beacon LED status for the route processor, fan-tray, power-supply slot, and slot for the selected switch.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
**hw-module switch slot**

To control components such as linecard or a supervisor available in a slot, use the **hw-module switch slot** command in the global configuration mode.

```
hw-module switch  switch-number slot  slot-number [logging onboard [counter | environment | message | poe | temperature | voltage] | shutdown ]
```

**Syntax Description**
- **switch-number**  The switch to access. Valid values are 1 and 2.
- **slot-number**  Specifies the slot number to access. Valid values are 1 to 4.
  - 1: Linecard slot 1
  - 2: Supervisor slot 0
  - 3: Supervisor slot 1
  - 4: Linecard slot 4
- **logging onboard**  Enables logging onboard.
- **counter**  (Optional) Configures the logging onboard counter.
- **environment**  (Optional) Configures the logging onboard environment.
- **message**  (Optional) Configures the logging onboard message.
- **poe**  (Optional) Configures the logging onboard PoE.
- **temperature**  (Optional) Configures the logging onboard temperature.
- **voltage**  (Optional) Configures the logging onboard voltage.
- **shutdown**  Shuts down a field-replaceable unit (FRU).

**Command Default**
None

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enable logging onboard for switch 1, slot 1:

```
Device# hw-module switch 1 slot 1 logging onboard
```

This example shows how to configure the logging onboard counter for switch 1, slot 1:
Device# `hw-module switch 1 slot 1 logging onboard counter`

This example shows how to configure the logging onboard environment for switch 1, slot 1:

Device# `hw-module switch 1 slot 1 logging onboard environment`

This example shows how to configure the logging onboard message for switch 1, slot 1:

Device# `hw-module switch 1 slot 1 logging onboard message`

This example shows how to configure the logging onboard PoE for switch 1, slot 1:

Device# `hw-module switch 1 slot 1 logging onboard poe`

This example shows how to configure the logging onboard temperature for switch 1, slot 1:

Device# `hw-module switch 1 slot 1 logging onboard temperature`

This example shows how to configure the logging onboard voltage for switch 1, slot 1:

Device# `hw-module switch 1 slot 1 logging onboard voltage`

This example shows how to shut down an FRU:

Device# `hw-module switch 1 slot 1 shutdown`
## hw-module switch usbflash

To unmount the USB SSD, use the `hw-module switch switch-number usbflash` command in privileged EXEC mode.

```
hw-module switch  switch-numberusbflashunmount
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch number</code></td>
<td>The switch to access. Valid values are 1 and 2.</td>
</tr>
<tr>
<td><code>usbflash unmount</code></td>
<td>Unmounts the USB SSD.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Global Configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Example

This example shows how to unmount the USB SSD from switch 1:

```
Device# hw-module switch 1 usbflash unmount
```
main-cpu

To enter the redundancy main configuration submode and enable the standby switch, use the main-cpu command in redundancy configuration mode.

main-cpu

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Redundancy configuration (config-red)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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#
maintenance-template

To create a maintenance template, use the `maintenance-template template_name` command in the global configuration mode. To delete the template, use the `no` form of the command.

```
maintenance-template template_name
no maintenance-template template_name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>maintenance-template</code></td>
<td>Creates a template for GIR with a specific name.</td>
</tr>
<tr>
<td><code>template_name</code></td>
<td>Name of the maintenance template.</td>
</tr>
</tbody>
</table>

### Command Default

Disabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.6.1</td>
<td></td>
</tr>
</tbody>
</table>

### Example:

The following example shows how to configure a maintenance template with the name `g1`:

```
Device(config)# maintenance template g1
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 (config-red)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show redundancy</strong></td>
<td>Displays redundancy facility information.</td>
</tr>
</tbody>
</table>
**reload**

To reload the stack member and to apply a configuration change, use the `reload` command in privileged EXEC mode.

```
reload [{/noverify | /verify}] [{/LINE | at | cancel | in | slot stack-member-number | standby-cpu}]
```

**Syntax Description**

- `/noverify` (Optional) Specifies to not verify the file signature before the reload.
- `/verify` (Optional) Verifies the file signature before the reload.
- `LINE` (Optional) Reason for the reload.
- `at` (Optional) Specifies the time in hh:mm for the reload to occur.
- `cancel` (Optional) Cancels the pending reload.
- `in` (Optional) Specifies a time interval for reloads to occur.
- `slot` (Optional) Saves the changes on the specified stack member and then restarts it.
- `stack-member-number` (Optional) Stack member number on which to save the changes. The range is 1 to 9.
- `standby-cpu` (Optional) Reloads the standby route processor (RP).

**Command Default**

Immediately reloads the stack member and puts a configuration change into effect.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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`
**router routing protocol shutdown l2**

To create instances that should be isolated within a maintenance template, use the `router routing_protocol instance_id | shutdown l2` command in the maintenance template configuration mode. To delete the instance, use the `no` form of the command.

```
{ router routing_protocol instance_id | shutdown l2 }
no { router routing_protocol instance_id | shutdown l2 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>router</code></td>
<td>Configures instance associated with routing protocol.</td>
</tr>
<tr>
<td><code>routing_protocol</code></td>
<td>Routing protocol defined for the template.</td>
</tr>
<tr>
<td><code>instance_id</code></td>
<td>Instance ID associated with the routing protocol.</td>
</tr>
<tr>
<td><code>shutdown l2</code></td>
<td>Configures instance to shut down layer 2 interfaces.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

Maintenance template configuration (config-maintenance-templ)

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to create an instance for ISIS with an instance ID of one under maintenance template `g1`:

```
Device(config)# maintenance template g1
Device(config-maintenance-templ)# router isis 1
```

The following example shows how to create an instance for shutting down layer 2 interfaces under maintenance template `g1`:

```
Device(config)# maintenance template g1
Device(config-maintenance-templ)# shutdown l2
```
set platform software fed switch

To set the packet cache count per SVL port, use the `set platform software fed switch` command in privileged EXEC or user EXEC mode.

```
set platform software fed switch {switch-number | active | standby} {F0 | F1 active} fss pak-cache count
```

**Syntax Description**

- `switch` Specifies information about the switch. You have the following options:
  - `switch-number`
  - `active` — Displays information relating to the active switch.
  - `standby` — Displays information relating to the standby switch, if available.

- `F0` Specifies information about the Embedded Service Processor slot 0.

- `FP active` Specifies information about the active Embedded Service Processor.

- `pak-cache count` Specifies the packet cache count. The range is 10 to 600. The default is 10.

**Command Default**

The default per port packet cache count is 10.

**Command Modes**

- User EXEC (>
- Privileged EXEC (#)

**Command History**

- **Release** Cisco IOS XE Gibraltar 16.10.1
  - **Modification** This command was introduced.

**Usage Guidelines**

None

**Example**

This example shows how to set the packet cache count per SVL port.

```
Device% set platform software fed switch active F1 active fss pak-cache 40
```
set platform software nif-mgr switch

To set the packet cache count per SVL port, use the `set platform software nif-mgr switch` command in privileged EXEC or user EXEC mode.

```
set platform software nif-mgr switch {switch-number | active | standby} R0 pak-cache count
```

**Syntax Description**

| switch {switch-number | active | standby} | Specifies information about the switch. You have the following options: |
|-------------------------------|------------------------------------------------------------------------------------------------|
| switch-number     | • switch-number                                                                                     |
| active            | • active — Displays information relating to the active switch.                                       |
| standby           | • standby — Displays information relating to the standby switch, if available.                      |

<table>
<thead>
<tr>
<th>R0</th>
<th>Specifies information about the Route Processor (RP) slot 0.</th>
</tr>
</thead>
<tbody>
<tr>
<td>pak-cache count</td>
<td>Specifies the packet cache count. The range is 10 to 600. The default is 10.</td>
</tr>
</tbody>
</table>

**Command Default**

The default per port packet cache count is 10.

**Command Modes**

- User EXEC(>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

**Example**

This example shows how to set the packet cache count per SVL port.

```
Device# set platform software nif_mgr switch active R0 pak-cache 40
```
show diagnostic bootup

To show the diagnostic boot information for a switch, use the show diagnostic bootup command in privileged EXEC mode.

`show diagnostic bootup level`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>level</th>
<th>Shows the diagnostic boot-level information.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Privileged EXEC (#)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

The following is a sample output of the `show diagnostic bootup level` command:

Device# show diagnostic bootup level

Current bootup diagnostic level: minimal
show diagnostic content

To show the diagnostic test content for a switch, use the **show diagnostic content** command in privileged EXEC mode.

**show diagnostic content switch**  \{**switch-number module**  \{1 \| 2 \| 4\} \| all \[all\]\}\}

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>switch switch-number</strong></td>
</tr>
<tr>
<td><strong>module</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td><strong>switch all</strong>  [all]</td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows a sample output of the **show diagnostic content switch all [all]** command.

Device# **show diagnostic content switch all all**

switch 1, module 1:

- Diagnostics test suite attributes:
  - M/C/* - Minimal bootup level test / Complete bootup level test / NA
  - B/* - Basic ondemand test / NA
  - P/V/* - Per port test / Per device test / NA
  - D/N/* - Disruptive test / Non-disruptive test / NA
  - S/* - Only applicable to standby unit / NA
  - X/* - Not a health monitoring test / NA
  - F/* - Fixed monitoring interval test / NA
  - E/* - Always enabled monitoring test / NA
  - A/I - Monitoring is active / Monitoring is inactive

| ID | Test Name | Attributes | Test Interval | Thre-
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1)</td>
<td>TestGoldPktLoopback</td>
<td><em>BPN</em>X**I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
</tbody>
</table>
2) TestPhyLoopback ------------------> *BPD*X**I not configured n/a
3) TestThermal -----------------------> *B*N****A 000 00:01:30.00 1
4) TestScratchRegister --------------> *B*N****A 000 00:01:30.00 5
5) TestPoe --------------------------> *B*N*X**I not configured n/a
6) TestUnusedPortLoopback ----------> *BPN****I not configured 1
7) TestPortTxMonitoring --------------> *BPN****A 000 00:01:15.00 1

switch 1, module 2:

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>Test Interval</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TestGoldPktLoopback</td>
<td><em>BPN</em>X**I</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>2</td>
<td>TestFantray</td>
<td><em>B</em>N****A</td>
<td>000 00:01:40.00 1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>TestPhyLoopback</td>
<td><em>BPD</em>X**I</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>4</td>
<td>TestThermal</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00 1</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TestScratchRegister</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00 5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TestMemory</td>
<td><em>B</em>D*X**I</td>
<td>not configured 1</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>TestUnusedPortLoopback</td>
<td><em>BPN</em>***I</td>
<td>not configured 1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>TestPortTxMonitoring</td>
<td><em>BPN</em>***A</td>
<td>000 00:01:15.00 1</td>
<td></td>
</tr>
</tbody>
</table>

switch 1, module 4:

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
D/N/* - Disruptive test / Non-disruptive test / NA
S/* - Only applicable to standby unit / NA
X/* - Not a health monitoring test / NA
F/* - Fixed monitoring interval test / NA
E/* - Always enabled monitoring test / NA
A/I - Monitoring is active / Monitoring is inactive

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>Test Interval</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TestGoldPktLoopback</td>
<td><em>BPN</em>X**I</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>2</td>
<td>TestPhyLoopback</td>
<td><em>BPD</em>X**I</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>3</td>
<td>TestThermal</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00 1</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>TestScratchRegister</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00 5</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>TestUnusedPortLoopback</td>
<td><em>BPN</em>***I</td>
<td>not configured 1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>TestPortTxMonitoring</td>
<td><em>BPN</em>***A</td>
<td>000 00:01:15.00 1</td>
<td></td>
</tr>
</tbody>
</table>

switch 2, module 1:

Diagnostics test suite attributes:
M/C/* - Minimal bootup level test / Complete bootup level test / NA
B/* - Basic ondemand test / NA
P/V/* - Per port test / Per device test / NA
### switch 2, module 2:

**Diagnostics test suite attributes:**
- **M/C/***: Minimal bootup level test / Complete bootup level test / NA
- **B/***: Basic ondemand test / NA
- **P/V/***: Per port test / Per device test / NA
- **D/N/***: Disruptive test / Non-disruptive test / NA
- **S/***: Only applicable to standby unit / NA
- **X/***: Not a health monitoring test / NA
- **F/***: Fixed monitoring interval test / NA
- **E/***: Always enabled monitoring test / NA
- **A/I**: Monitoring is active / Monitoring is inactive

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>Test Interval Thre-</th>
<th>Thre-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>day hh:mm:ss.ms shold</td>
<td></td>
</tr>
<tr>
<td>1)</td>
<td>TestGoldPktLoopback</td>
<td><em>BPN</em>X**I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>2)</td>
<td>TestPhyLoopback</td>
<td><em>BPD</em>X**I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>3)</td>
<td>TestThermal</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00</td>
<td>1</td>
</tr>
<tr>
<td>4)</td>
<td>TestScratchRegister</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00</td>
<td>5</td>
</tr>
<tr>
<td>5)</td>
<td>TestPoe</td>
<td><em>B</em>N<strong>X</strong>I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>6)</td>
<td>TestUnusedPortLoopback</td>
<td><em>BPN</em>***I</td>
<td>not configured</td>
<td>1</td>
</tr>
<tr>
<td>7)</td>
<td>TestPortTxMonitoring</td>
<td><em>BPN</em>***A</td>
<td>000 00:01:15.00</td>
<td>1</td>
</tr>
</tbody>
</table>

### switch 2, module 4:

**Diagnostics test suite attributes:**
- **M/C/***: Minimal bootup level test / Complete bootup level test / NA
- **B/***: Basic ondemand test / NA
- **P/V/***: Per port test / Per device test / NA
- **D/N/***: Disruptive test / Non-disruptive test / NA
- **S/***: Only applicable to standby unit / NA
- **X/***: Not a health monitoring test / NA
- **F/***: Fixed monitoring interval test / NA
- **E/***: Always enabled monitoring test / NA
- **A/I**: Monitoring is active / Monitoring is inactive

<table>
<thead>
<tr>
<th>ID</th>
<th>Test Name</th>
<th>Attributes</th>
<th>Test Interval Thre-</th>
<th>Thre-</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>day hh:mm:ss.ms shold</td>
<td></td>
</tr>
<tr>
<td>1)</td>
<td>TestGoldPktLoopback</td>
<td><em>BPN</em>X**I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>2)</td>
<td>TestPhyLoopback</td>
<td><em>BPD</em>X**I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>3)</td>
<td>TestThermal</td>
<td><em>B</em>N****A</td>
<td>000 00:01:30.00</td>
<td>1</td>
</tr>
<tr>
<td>4)</td>
<td>TestPoe</td>
<td><em>B</em>N<strong>X</strong>I</td>
<td>not configured</td>
<td>n/a</td>
</tr>
<tr>
<td>5)</td>
<td>TestUnusedPortLoopback</td>
<td><em>BPN</em>***I</td>
<td>not configured</td>
<td>1</td>
</tr>
<tr>
<td>6)</td>
<td>TestPortTxMonitoring</td>
<td><em>BPN</em>***A</td>
<td>000 00:01:15.00</td>
<td>1</td>
</tr>
</tbody>
</table>
4) TestScratchRegister -------------> *B*N****A 000 00:01:30.00 5
5) TestUnusedPortLoopback ---------> *BPN****I not configured 1
6) TestPortTxMonitoring -------------> *BPN****A 000 00:01:15.00 1
show diagnostic description

To show the diagnostic test description for a switch, use the `show diagnostic description` command in privileged EXEC mode.

```
show diagnostic description switch {switch-number module {1 | 2 | 4} test {test-id | all} |
all test {test-list | test-id | all}}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch switch-number</code></td>
<td>Specifies the switch to be selected.</td>
</tr>
<tr>
<td><code>switch all</code></td>
<td>Selects all the switches.</td>
</tr>
<tr>
<td><code>module</code></td>
<td>Selects a module of the switch.</td>
</tr>
<tr>
<td><code>1</code></td>
<td>Selects the module C9400-LC-48U.</td>
</tr>
<tr>
<td><code>2</code></td>
<td>Selects the module C9400-SUP-1.</td>
</tr>
<tr>
<td><code>4</code></td>
<td>Selects the module C9400-LC-48T.</td>
</tr>
<tr>
<td><code>test test-id</code></td>
<td>Displays the diagnostic test description for the test ID or test name specified.</td>
</tr>
<tr>
<td><code>test test-list</code></td>
<td>Displays the diagnostic test description for the list of test IDs specified.</td>
</tr>
<tr>
<td><code>test all</code></td>
<td>Displays the diagnostic test description for all the test IDs.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows sample output of the `show diagnostic description switch switch-number module 4 test all` command:

```
Device# show diagnostic description switch 1 module 4 test all

TestGoldPktLoopback:
The GOLD packet Loopback test verifies the MAC level loopback functionality. In this test, a GOLD packet, for which doppler provides the support in hardware, is sent. The packet loops back at MAC level and is matched against the stored packet. It is a non-disruptive test.

TestPhyLoopback:
The PHY Loopback test verifies the PHY level loopback functionality. In this test, a packet is sent which loops back at PHY level and is matched against the stored packet. It is a disruptive test and cannot be run as a health monitoring test.
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
TestThermal:
This test verifies the temperature reading from the sensor is below the yellow temperature threshold. It is a non-disruptive test and can be run as a health monitoring test.

TestScratchRegister:
The Scratch Register test monitors the health of application-specific integrated circuits (ASICs) by writing values into registers and reading back the values from these registers. It is a non-disruptive test and can be run as a health monitoring test.

TestUnusedPortLoopback:
This test verifies the PHY level loopback functionality for admin-down ports. In this test, a packet is sent which loops back at PHY level and is matched against the stored packet. It is a non-disruptive test and can be run as a health monitoring test.

TestPortTxMonitoring:
This test monitors the TX counters of a connected interface. This test verifies if the connected port is able to send the packets or not. It is a non-disruptive test and can be run as a health monitoring test.
**show diagnostic events**

To show the diagnostic event log for a switch, use the `show diagnostic events` command in privileged EXEC mode.

```
show diagnostic events switch {switch-number module {1 | 2 | 4} | all [event-type [error | info | warning]]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch-number</td>
<td>Specifies the switch to be selected.</td>
</tr>
<tr>
<td>switch all</td>
<td>Selects all the switches.</td>
</tr>
<tr>
<td>module</td>
<td>Selects a module of the switch.</td>
</tr>
<tr>
<td>1</td>
<td>Displays diagnostic event logs for the C9400-LC-48U module.</td>
</tr>
<tr>
<td>2</td>
<td>Displays diagnostic event logs for the C9400-SUP-1 module.</td>
</tr>
<tr>
<td>4</td>
<td>Displays diagnostic event logs for the C9400-LC-48T module.</td>
</tr>
<tr>
<td>event-type</td>
<td>(Optional) Displays the event log of a specific event type. The following are the valid values:</td>
</tr>
<tr>
<td>• error</td>
<td>Displays the error type event logs.</td>
</tr>
<tr>
<td>• info</td>
<td>Displays the information type event logs.</td>
</tr>
<tr>
<td>• warning</td>
<td>Displays the warning type event logs.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows a sample output of the `show diagnostic events switch switch-number module` command.

```
Device# show diagnostic events switch 1 module 2

Diagnostic events (storage for 500 events, 500 events recorded)
Number of events matching above criteria = 500
Event Type (ET): I - Info, W - Warning, E - Error

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>ET</th>
<th>Card</th>
<th>Event Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/08 13:54:05.110</td>
<td>E</td>
<td>[1-2]</td>
<td>TestThermal Failed</td>
</tr>
</tbody>
</table>
```
07/08 14:00:05.614 E [1-2] TestThermal Failed
07/08 14:01:35.615 E [1-2] TestThermal Failed
07/08 14:03:05.616 E [1-2] TestThermal Failed
07/08 14:04:36.367 E [1-2] TestThermal Failed
07/08 14:06:06.368 E [1-2] TestThermal Failed
07/08 14:07:37.370 E [1-2] TestThermal Failed
07/08 14:10:38.372 E [1-2] TestThermal Failed
07/08 14:12:10.873 E [1-2] TestThermal Failed
<Output truncated>
show diagnostic result

To show the diagnostic test result information, use the `show diagnostic result` command in privileged EXEC mode.

```
show diagnostic result switch (switch-number module { 1 | 2 | 4 }) (detail | failure [ detail ] | test { test-id | all } [ detail ] | xml | all [ all [ detail | failure [ detail ] ] ] )
```

**Syntax Description**

- `switch switch-number` Specifies the switch to be selected.
- `module` Selects a module of the switch.
- `1` Displays the diagnostic test results for the module C9400-LC-48U.
- `2` Displays the diagnostic test results for the module C9400-SUP-1.
- `4` Displays the diagnostic test results for the module C9400-LC-48T.
- `detail` (Optional) Displays the detailed test results.
- `failure` (Optional) Displays the failed test results.
- `test test-id` (Optional) Displays the diagnostic test results for the selected test ID or test name or list of test IDs of a module.
- `test all` (Optional) Displays the diagnostic test results for all the tests of a module.
- `xml` (Optional) Displays the test results in XML format.
- `switch all` [ all ]
  - `switch all`—Displays the diagnostic test results for all the switches.
  - (Optional) all—Displays the diagnostic test results for all the cards of all the switches.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example displays sample output of the `show diagnostic result switch switch-number module 4 [ failure [ detail ] ]` command:
Device# `show diagnostic result switch 1 module 4 failure detail`

Current bootup diagnostic level: minimal

switch 1, module 4: SerialNo : JAE204700PH

Overall Diagnostic Result for switch 1, module 4 : PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

This example displays sample output for the `show diagnostic result switch switch-number module module-number detail` command.

Device# `show diagnostic result switch 1 module 4 detail`

Current bootup diagnostic level: minimal

switch 1, module 4: SerialNo : JAE204700PH

Overall Diagnostic Result for switch 1, module 4 : PASS
Diagnostic level at card bootup: minimal

Test results: (. = Pass, F = Fail, U = Untested)

1) TestGoldPktLoopback:

| Port | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|      | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |
| Port | 25| 26| 27| 28| 29| 30| 31| 32| 33| 34| 35| 36| 37| 38| 39| 40| 41| 42| 43| 44| 45| 46| 47| 48|    |
|      | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count -------------> 0
Last test testing type -------> n/a
Last test execution time -----> n/a
First test failure time ------> n/a
Last test failure time ------> n/a
Last test pass time ----------> n/a
Total failure count ----------> 0
Consecutive failure count ---> 0

2) TestPhyLoopback:

| Port | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
|      | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |
| Port | 25| 26| 27| 28| 29| 30| 31| 32| 33| 34| 35| 36| 37| 38| 39| 40| 41| 42| 43| 44| 45| 46| 47| 48|    |
|      | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U | U |

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count --------------> 0
Last test testing type -------> n/a
3) TestThermal ----------------- .

Error code ------------------> 0 (DIAG_SUCCESS)
Total run count --------------> 1771
Last test testing type -------> Health Monitoring
Last test execution time ----> Jul 09 2018 03:06:53
First test failure time -----> n/a
Last test failure time -------> n/a
Last test pass time ---------> Jul 09 2018 03:06:53
Total failure count ---------> 0
Consecutive failure count ---> 0

4) TestScratchRegister ----------- .

Error code ------------------> 0 (DIAG_SUCCESS)
Total run count --------------> 1771
Last test testing type -------> Health Monitoring
Last test execution time ----> Jul 09 2018 03:06:53
First test failure time -----> n/a
Last test failure time -------> n/a
Last test pass time ---------> Jul 09 2018 03:06:53
Total failure count ---------> 0
Consecutive failure count ---> 0

5) TestUnusedPortLoopback:

Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
----------------------------------------------------------------------------
  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
----------------------------------------------------------------------------
  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U

Error code ------------------> 3 (DIAG_SKIPPED)
Total run count --------------> 0
Last test testing type -------> n/a
Last test execution time ----> n/a
First test failure time -----> n/a
Last test failure time -------> n/a
Last test pass time ---------> n/a
Total failure count ---------> 0
Consecutive failure count ---> 0

6) TestPortTxMonitoring:

Port  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
----------------------------------------------------------------------------
  . U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
Port 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48
----------------------------------------------------------------------------
This example displays sample output for the `show diagnostic result switch switch-number module 4 [test [test-id]]` command.

```
Device# show diagnostic result switch 1 module 4 test 3

Current bootup diagnostic level: minimal

Test results: (. = Pass, F = Fail, U = Untested)

   3) TestThermal ------------------> .

Switch#show diagnostic result switch 1 module 4 test 3 detail ?
| Output modifiers
<cr> <cr>
Switch#show diagnostic result switch 1 module 4 test 3 detail

Current bootup diagnostic level: minimal

Test results: (. = Pass, F = Fail, U = Untested)

   3) TestThermal ------------------> .
```

This example displays sample output for the `show diagnostic result switch switch-number module 4 [xml]` command.

```
Device# show diagnostic result switch 1 module 4 xml

Current bootup diagnostic level: minimal

<?xml version="1.0" ?>
<diag>
<diag_results>
<diag_info>
This file report diag test results
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
<diag_info>
<result overall_result="DIAG_PASS" new_failure="FALSE" diag_level="DIAG_LEVEL_MINIMAL" />
<card name="switch 1, module 4" index="3198" serial_no="JAE204700PH" >
<card_no>
9
</card_no>
<total_port>
48
</total_port>
@test name="TestGoldPktLoopback" >
@test_result>
<portmask>
00000000-00000000-00000000-00000000-00000000-00000000-11111111-11111111-11111111
</portmask>
<per_port_result result="DIAG_RESULT_UNKNOWN" port="1" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="2" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="3" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="4" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="5" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="6" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="7" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="8" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="9" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="10" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="11" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="12" />
<per_port_result result="DIAG_RESULT_UNKNOWN" port="13" />
</Output truncated>
show diagnostic simulation failure

To display the diagnostic failure simulation information for a card on a switch, use the `show diagnostic simulation failure` command in privileged EXEC mode.

```
show diagnostic simulation failure switch {switch-number module {1 | 2 | 4} | all [all]}
```

### Syntax Description

- **switch switch-number**: Specifies the switch to be selected.
- **module**: Selects a module of the switch.
- **1**: Displays diagnostic failure simulation information for the C9400-LC-48U module.
- **2**: Displays diagnostic failure simulation information for the C9400-SUP-1 module.
- **4**: Displays diagnostic failure simulation information for the C9400-LC-48T module.
- **switch all [all]**: Selects all the switches.
-  
  - **(Optional) all**: Displays all the diagnostic failure simulation information for all the switches.

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

This example shows sample output of the `show diagnostic simulation failure switch all` command:

```
Device# show diagnostic simulation failure switch all

There is no test failure simulation installed.
```
show diagnostic schedule

To display the diagnostic schedule information for a card on a switch, use the show diagnostic schedule command in privileged EXEC mode.

show diagnostic schedule switch  {switch-number module {1 | 2 | 4} | all [all] }

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch-number</td>
<td>Specifies the switch to be selected.</td>
</tr>
<tr>
<td>module</td>
<td>Selects a module of the switch.</td>
</tr>
<tr>
<td>1</td>
<td>Displays diagnostic schedule information for the C9400-LC-48U module.</td>
</tr>
<tr>
<td>2</td>
<td>Displays diagnostic schedule information for the C9400-SUP-1 module.</td>
</tr>
<tr>
<td>4</td>
<td>Displays diagnostic schedule information for the C9400-LC-48T module.</td>
</tr>
<tr>
<td>switch all</td>
<td>Selects all switches.</td>
</tr>
<tr>
<td>[all]</td>
<td>(Optional)all—Displays all the diagnostic schedule information for all the switches.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

This example shows sample output of the show diagnostic schedule switch  switch-number  module 2 command:

Device# show diagnostic schedule switch 1 module 2

Current Time = 03:14:24 PDT Mon Jul 9 2018

Diagnostic for switch 1, module 2 is not scheduled.
show hw-module switch subslot

To display information for all the supported modules in the system and chassis location information, use the `show hw-module switch switch-number subslot` command in privileged EXEC mode. To disable this feature, use the `no` form of this command.

```
show hw-module switch switch-number subslot
(slot/subslot | all | attribute | entity | oir | sensors [limits] | subblock | tech-support)
```

```
noshow hw-module switch switch-number subslot
(slot/subslot | all | attribute | entity | oir | sensors [limits] | subblock | tech-support)
```

**Syntax Description**

- `switch number`: Specifies the switch to access; valid values are 1 and 2.
- `subslot slot/subslot`: Specifies module slot or subslot number.
  - Valid values for slot are 1 to 4.
  - Valid value for subslot is 0.
- `all`: Selects all the supported modules in the subslot level.
- `attribute`: Displays module attribute information.
- `entity`: Displays entity MIB details.
  - **Note**: Not intended for production use.
- `oir`: Displays online insertion and removal (OIR) summary.
- `sensors`: Displays environmental sensor summary.
- `limits`: Displays sensor limits.
- `subblock`: Displays subblock details.
  - **Note**: Not intended for production use.
- `tech-support`: Displays subslot information for technical support.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to obtain module attribute information for switch 1 for all the modules in the subslot level:
Device# show hw-module switch 1 subslot all attribute

This example shows how to obtain module OIR information for switch 1 for all the modules in the subslot level:

Device# show hw-module switch 1 subslot all oir

This example shows how to obtain environmental sensor summary for switch 1 for all the modules in the subslot level:

Device# show hw-module switch 1 subslot all sensors

This example shows how to obtain sensory limits information for switch 1 for all modules in the subslot level:

Device# show hw-module switch 1 subslot all sensors limit

This example shows how to obtain subslot information for technical support for switch 1 for all modules in the subslot level:

Device# show hw-module switch 1 subslot all tech-support
show logging onboard switch

To display the on-board failure logging (OBFL) information of a switch, use the `show logging onboard switch` command in privileged EXEC mode.

```
show logging onboard switch
  {switch-number | active | standby} (RP {standby | active})
  slot {1 | 4 | F0 | F1 | R0 | R1} {clilog | counter | environment | message | poe
  | temperature | uptimevo | voltage} {continuous | detail | summary} [start hh:mm:ss day
  month year] [end hh:mm:ss day month year] } | state | status
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch-number</td>
<td>Switch for which OBFL information is displayed.</td>
</tr>
<tr>
<td>active</td>
<td>Displays OBFL information about the active switch.</td>
</tr>
<tr>
<td>standby</td>
<td>Displays OBFL information about the standby switch.</td>
</tr>
<tr>
<td>RP</td>
<td>Specifies the route processor (RP).</td>
</tr>
<tr>
<td>slot</td>
<td>Specifies the slot information.</td>
</tr>
<tr>
<td>clilog</td>
<td>Displays the OBFL commands that were entered on the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>counter</td>
<td>Displays the counter of the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>environment</td>
<td>Displays the unique device identifier (UDI) information for the standalone switch or specified stack members. Also displays the product identification (PID), the version identification (VID), and the serial number for all the connected FRU devices.</td>
</tr>
<tr>
<td>message</td>
<td>Displays the hardware-related system messages generated by the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>poe</td>
<td>Displays the power consumption of the Power over Ethernet (PoE) ports on the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>state</td>
<td>Displays the state of the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>status</td>
<td>Displays the status of the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>temperature</td>
<td>Displays the temperature of the standalone switch or specified stack members.</td>
</tr>
<tr>
<td>uptime</td>
<td>Displays the time at which the standalone switch or specified stack members start, the reason the standalone switch or specified members restart, and the length of time the standalone switch or specified stack members have been running since they last restarted.</td>
</tr>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Command History</td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When OBFL is enabled, the switch records the OBFL data in a continuous file that contains all the data. The continuous file is circular. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file. Creating the summary file frees up space in the continuous file so that the switch can write newer data to it.

Use the `start` and `end` keywords to display the data collected only during a particular time period.

**Examples**

This is a sample output of the `show logging onboard switch 1 RP active message` command:

```
Device# show logging onboard switch 1 RP active message

ERROR MESSAGE SUMMARY INFORMATION

MM/DD/YYYY HH:MM:SS Facility-Sev-Name | Count | Persistence Flag
--------------------------------------------------------------------------------------
07/06/2018 00:45:23 %IOSXE-2-DIAGNOSTICS_FAILED : >254 LAST Diagnostics Thermal failed
07/06/2018 00:19:57 %IOSXE-2-DIAGNOSTICS_PASSED : >254 LAST Diagnostics Fantray passed
07/07/2018 11:36:10 %IOSXE-2-TRANSCEIVER_INSERTED : >254 LAST Transceiver module inserted in TenGigabitEthernet1/2/0/5
05/03/2018 05:49:57 %IOSXE-2-TRANSCEIVER_REMOVED : 82 : LAST : Transceiver module removed from TenGigabitEthernet1/2/0/7
```

**Syntax**

- `voltage` (Optional) Displays the system voltages of the standalone switch or the specified switch stack members.
- `continuous` (Optional) Displays the data in the continuous file.
- `detail` (Optional) Displays both the continuous and summary data.
- `summary` (Optional) Displays the data in the summary file.
- `start hh:mm:ss day month year` (Optional) Displays the data from the specified time and date. Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colon (:`), for example, 13:32:45. The range of day is from 1 to 31. The month in uppercase or lower case letters. You can enter the full name of the month, such as January or august, or the first three letters of the month, such as Jan or Aug. The year is a 4-digit number, such as 2008. The range is from 1970 to 2099.
- `end hh:mm:ss day month year` (Optional) Displays the data up to the specified time and date. Enter the time as a 2-digit number for a 24-hour clock. Make sure to use the colon (:`), for example, 13:32:45. The range of day is from 1 to 31. The month in uppercase or lower case letters. You can enter the full name of the month, such as January or August, or the first three letters of the month, such as Jan or Aug. The year is a 4-digit number, such as 2008. The range is from 1970 to 2099.
This is a sample output of the `show logging onboard switch 1 slot 4 status` command:

```
Device# show logging onboard switch 1 slot 4 status
```

```
OBFL Application Status

Application Uptime:
  Path: /obfl0/
  Cli enable status: enabled

Application Message:
  Path: /obfl0/
  Cli enable status: enabled

Application Voltage:
  Path: /obfl0/
  Cli enable status: enabled

Application Temperature:
  Path: /obfl0/
  Cli enable status: enabled

Application POE:
  Path: /obfl0/
  Cli enable status: enabled

Application Environment:
  Path: /obfl0/
  Cli enable status: enabled

Application Counter:
  Path: /obfl0/
  Cli enable status: enabled

Application Clilog:
  Path: /obfl0/
  Cli enable status: enabled
```

This is a sample output of the `show logging onboard switch 1 slot 4 state` command:

```
Device# show logging onboard switch 1 slot 4 state
GREEN
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear logging onboard</td>
<td>Removes the OBFL data from flash memory.</td>
</tr>
<tr>
<td>hw-module logging onboard</td>
<td>Enables OBFL.</td>
</tr>
</tbody>
</table>
show platform software fed

To display the per port SDP/LMP control packet exchange history between FED and Network Interface Manager (NIF Mgr) software processes, use the `show platform software fed` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} fss {counters | interface-counters interface {interface-type interface-number} | lmp-packets interface {interface-type interface-number} | sdp-packets
```

**Syntax Description**

- **switch {switch-number | active | standby}**
  - Displays information about the switch. You have the following options:
    - `switch-number`
    - `active`—Displays information relating to the active switch.
    - `standby`—Displays information relating to the standby switch, if available.
  - **Note** This keyword is not supported.

- **fss**
  - Specifies information about Front Side Stacking (FSS).

- **counters**
  - Displays the number of TX and RX packets of SDP, LMP, OOB1/2, EMP and LOOPBACK types.

- **interface-counters**
  - Displays the number of TX and RX packets for all the interfaces. You can filter the output to display for a particular SVL interface using the `interface-counters interface {interface-type interface-number}` command.

- **lmp-packets**
  - Displays details of LMP packet transactions between FED and NIF Manager for all the SVL interfaces. You can filter the output to display for a particular SVL interface using the `lmp-packets interface {interface-type interface-number}` command.

- **sdp-packets**
  - Displays details of SDP packets transmitted between FED and NIF Manager for all the SVL interfaces.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

- **Release**
  - **Modification**
  - Cisco IOS XE Gibraltar 16.10.1 This command was introduced.

**Usage Guidelines**

By default, the output of `show platform software fed switch active fss sdp-packets` command displays a packet cache count of 10. You can set the packet cache count per port to a maximum of 600 using the `set platform software fed switch` command.
Example

The following is sample output from the `show platform software fed switch active fss lmp-packets interface interface-type interface-number` command.

```
Device# show platform software fed switch active fss lmp-packets interface fortygigabitethernet1/0/1

Interface: fortygigabitethernet1/0/1 IFID:0x1d
FED FSS LMP packets max 10:

FED --> Nif Mgr
Timestamp LPN LPN Seq
-------------------------------------------------------
Tue Sep 18 12:45:13 2018 11 11 4329
Tue Sep 18 12:45:14 2018 11 11 4330
```

The following is sample output from the `show platform software fed switch active fss sdp-packets` command.

```
Device# show platform software fed switch active fss sdp-packets
FED FSS SDP packets max 10:

FED-> Nif Mgr
Timestamp Src Mac Dst Mac Seq Num
---------------------------------------------------------------------------------------------------------
Thu Oct 4 05:54:04 2018 e4aa:5d54:8aa8 ffff:ffff:ffff 262
Thu Oct 4 05:54:08 2018 e4aa:5d54:8aa8 ffff:ffff:ffff 263
Thu Oct 4 05:54:12 2018 e4aa:5d54:8aa8 ffff:ffff:ffff 264
```

The following is sample output from the `show platform software fed switch active fss counters` command.

```
Device# show platform software fed switch active fss counters
FSS Packet Counters

                   SDP                LMP
                   TX | RX TX | RX
--------------------- ---------------------
 1493 1494 4988 4988

                   OOB1                OOB2
                   TX | RX TX | RX
--------------------- ---------------------
 22 8 134858 133833

                   EMP                LOOPBACK
                   TX | RX
--------------------- -------------------
 0 0 71
```

The following is sample output from the `show platform software fed switch active fss interface-counters interface interface-type interface-number` command.

```
Device# show platform software fed switch active fss interface-counters interface fortygigabitethernet1/0/1

```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Interface fortygigabitethernet1/0/1 IFID: 0x1d Counters

<table>
<thead>
<tr>
<th>LMP</th>
<th>TX</th>
<th>RX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6391</td>
<td>6389</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set platform software fed switch</td>
<td>Configures the per port packet cache count for an SVL interface.</td>
</tr>
</tbody>
</table>
show platform software nif-mgr switch

To display the control packet exchange history between the Network Interface Manager software process (NIF Mgr) and the StackWise Virtual Link (SVL) interfaces, use the `show platform software nif-mgr switch` command in privileged EXEC mode.

```
show platform software nif-mgr switch {switch-number | active | standby} R0 {counters [lpn lpn-index] | packets [lpn lpn-index] | switch-info}
```

```
show platform software nif-mgr switch {switch-number | active | standby} R0 {counters [slotslot-number] | portsport-number | packets [slotslot-number] | portsport-number} {switch-info}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`switch {switch-number</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>• <code>switch-number</code></td>
</tr>
<tr>
<td></td>
<td>• <code>active</code> — Displays information relating to the active switch.</td>
</tr>
<tr>
<td></td>
<td>• <code>standby</code> — Displays information relating to the standby switch, if available.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This keyword is not supported.</td>
</tr>
<tr>
<td><code>R0</code></td>
<td>Displays information about the Route Processor (RP) slot 0.</td>
</tr>
<tr>
<td><code>counters</code></td>
<td>Displays the number of TX and RX packets of LMP and SDP type.</td>
</tr>
<tr>
<td><code>lpn lpn-index</code></td>
<td>Specifies the local port number (LPN). The range is 1 to 96.</td>
</tr>
<tr>
<td></td>
<td>Use the <code>show platform software nif-mgr switch active R0 switch-info</code> command for information about <code>lpn-index</code>.</td>
</tr>
<tr>
<td><code>switch-info</code></td>
<td>Displays information about NIF Manager operational database.</td>
</tr>
<tr>
<td><code>packets</code></td>
<td>Displays the details of TX and RX packets of LMP and SDP type.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of the `show platform software nif-mgr switch active R0 counters` command displays counters for LMP and SDP packets that are transmitted.

The output of the `show platform software nif-mgr switch active R0 switch-info` command displays the SVL links details and the protocol flap count on each of the links.

- **LMP to FED**
• SDP to FED
• FED to LMP
• FED to SDP
• Stack Manager to SDP
• SDP to Stack Manager

The output of the **show platform software nif-mgr switch active R0 packets** command displays the timestamp details of the LMP and SDP packets transmitted.

• Timestamp of last 10 LMP frames from FED
• Timestamp of last 10 LMP frames to FED
• Timestamp of last 10 SDP frames from Stack manager
• Timestamp of last 10 SDP frames to Stack manager

By default, the packet cache count per SVL port during bootup is 10. To set the packet cache count per port, use the **set platform software nif-mgr switch** command.

**Example**

The following is sample output from the **show platform software nif-mgr switch active R0 counters** command.

```
Device# show platform software nif-mgr switch active R0 counters
NIF Manager Counters
    Counters:                                             
    Stack Link : 1                                        
    FED to NIF Mgr                                        
    -------------------------------
    Number of LMP RX Packets : 749
    NIF Mgr to FED                                        
    -------------------------------
    Number of LMP TX Packets : 758
    Stack Link : 2                                        
    FED to NIF Mgr                                        
    -------------------------------
    Number of LMP RX Packets : 0
    NIF Mgr to FED                                        
    -------------------------------
    Number of LMP TX Packets : 0
    NIF Mgr to Stack Mgr
    -------------------------------
    Number of SDP Success Packets - 1854
    Number of SDP Fail Packets - 0
    Stack Mgr to NIF Mgr
    -------------------------------
    Number of SDP Success Packets - 1850
    Number of SDP Fail Packets - 0
```
The following is sample output from the `show platform software nif-mgr switch active R0 counters lpn lpn-index` command.

```
Device# show platform software nif_mgr switch active r0 counters lpn 1
Counters:
#############################################################
LPN : 1 Stack Link : 1 port 1
===============================================
FED to NIF Mgr
-------------
Number of LMP RX Packets : 760
NIF Mgr to FED
-------------
Number of LMP TX Packets : 768
```

The following is sample output from the `show platform software nif-mgr switch active R0 packets` command.

```
Device# show platform software nif-mgr switch active R0 packets
NIF manager packets max 10:
Stack Link : 1
LMP
----------
FED->
Nif Mgr
Timestamp Local Peer Seq LPN LPN Num
--------------------------------------------------------
Wed Jun 20 02:20:49 2018 3 3 1050
Wed Jun 20 02:20:50 2018 3 3 1051
Wed Jun 20 02:20:41 2018 3 3 1042
Wed Jun 20 02:20:42 2018 3 3 1043
Wed Jun 20 02:20:43 2018 3 3 1044
Wed Jun 20 02:20:44 2018 3 3 1045
Wed Jun 20 02:20:45 2018 3 3 1046
Wed Jun 20 02:20:46 2018 3 3 1047
Wed Jun 20 02:20:47 2018 3 3 1048
Wed Jun 20 02:20:48 2018 3 3 1049
Nif Mgr->
FED
Timestamp Local Peer Seq LPN LPN Num
--------------------------------------------------------
Wed Jun 20 02:20:49 2018 3 3 1050
Wed Jun 20 02:20:50 2018 3 3 1051
Wed Jun 20 02:20:41 2018 3 3 1042
Wed Jun 20 02:20:42 2018 3 3 1043
Wed Jun 20 02:20:43 2018 3 3 1044
Wed Jun 20 02:20:44 2018 3 3 1045
Wed Jun 20 02:20:45 2018 3 3 1046
Wed Jun 20 02:20:46 2018 3 3 1047
Wed Jun 20 02:20:47 2018 3 3 1048
Wed Jun 20 02:20:48 2018 3 3 1049
SDP
-----------
Nif Mgr->
Stack Mgr
Timestamp Src Mac Dst Mac Seq Num
------------------------------------------------------------------------
Wed Jun 20 02:20:40 2018 40ce:2499:aa90 ffff:ffff:ffff 320
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set platform software nif-mgr switch</td>
<td>Configures the per port packet cache count for an SVL interface.</td>
</tr>
</tbody>
</table>
show redundancy

To display redundancy facility information, use the `show redundancy` command in privileged EXEC mode.

```plaintext
show redundancy [{clients | config-sync | counters | history [{reload | reverse}] | slaves[slave-name] clients | counters} | states | switchover history [domain default]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clients</code></td>
<td>(Optional) Displays information about the redundancy facility client.</td>
</tr>
<tr>
<td><code>config-sync</code></td>
<td>(Optional) Displays a configuration synchronization failure or the ignored mismatched command list (MCL). For more information, see <code>show redundancy config-sync</code>, on page 127.</td>
</tr>
<tr>
<td><code>counters</code></td>
<td>(Optional) Displays information about the redundancy facility counter.</td>
</tr>
<tr>
<td><code>history</code></td>
<td>(Optional) Displays a log of past status and related information for the redundancy facility.</td>
</tr>
<tr>
<td><code>history reload</code></td>
<td>(Optional) Displays a log of past reload information for the redundancy facility.</td>
</tr>
<tr>
<td><code>history reverse</code></td>
<td>(Optional) Displays a reverse log of past status and related information for the redundancy facility.</td>
</tr>
<tr>
<td><code>slaves</code></td>
<td>(Optional) Displays all slaves in the redundancy facility.</td>
</tr>
<tr>
<td><code>slave-name</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>clients</code></td>
<td>Displays all redundancy facility clients in the specified slave.</td>
</tr>
<tr>
<td><code>counters</code></td>
<td>Displays all counters in the specified slave.</td>
</tr>
<tr>
<td><code>states</code></td>
<td>(Optional) Displays information about the redundancy facility state, such as disabled, initialization, standby or active.</td>
</tr>
<tr>
<td><code>switchover history</code></td>
<td>(Optional) Displays information about the redundancy facility switchover history.</td>
</tr>
<tr>
<td><code>domain default</code></td>
<td>(Optional) Displays the default domain as the domain to display switchover history for.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to display information about the redundancy facility:

```plaintext
Device# show redundancy
Redundant System Information:
```

---

*Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)*
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 DEPLOYMENT ENGINEERING NOVA WEEKLY BUILD, synced to DSGS_PI2_POSTPC_FLO_DSBU7_NG3K_1105
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_APPROGUE
  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 = 129 clientSeq = 60 Redundancy Mode RF
  clientID = 139 clientSeq = 61 IfIndex
  clientID = 3300 clientSeq = 62 Persistent Variable
  clientID = 25 clientSeq = 68 CHKPT RF
  clientID = 20005 clientSeq = 74 IIF-shim
  clientID = 10001 clientSeq = 82 QEMU Platform RF

<output truncated>

The output displays the following information:

• clientID displays the client’s ID number.
• clientSeq displays the client’s notification sequence number.
• Current redundancy facility state.
This example shows how to display the redundancy facility counter information:

```
Device# show redundancy counters
Redundancy Facility OMs
    comm link up = 0
    comm link down = 0
    invalid client tx = 0
    null tx by client = 0
    tx failures = 0
    tx msg length invalid = 0
    client not rxing msgs = 0
    rx peer msg routing errors = 0
    null peer msg rx = 0
    errored peer msg rx = 0
    buffers tx = 0
    tx buffers unavailable = 0
    buffers rx = 0
    buffer release errors = 0
    duplicate client registers = 0
    failed to register client = 0
    Invalid client syncs = 0
```

Device#

This example shows how to display redundancy facility history information:

```
Device# show redundancy history
00:00:00 *my state = INITIALIZATION(2) peer state = DISABLED(1)
00:00:00 RF_EVENT_INITIALIZATION(524) op=0 rc=0
00:00:00 *my state = NEGOTIATION(3) peer state = DISABLED(1)
00:00:01 client added: Table Manager Client(24001) seq=21
00:00:01 client added: SNMP SA HA Client(20010) seq=24
00:00:06 client added: WCM_CAPWAP(24100) seq=5
00:00:06 client added: WCM_QOS HA(24103) seq=8
00:00:07 client added: WCM_DOT1X(24106) seq=11
00:00:07 client added: EICORE HA Client(20002) seq=4
00:00:09 client added: WCM_MOBILITY(24105) seq=10
00:00:09 client added: WCM_NETFLOW(24111) seq=16
00:00:09 client added: WCM_APFROGUE(24107) seq=12
00:00:09 client added: WCM_RRM HA(24101) seq=6
00:00:09 client added: WCM_MCAST(24112) seq=17
00:00:09 client added: WCM_CIDSW(24110) seq=15
00:00:09 client added: bcm_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**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>failures</td>
<td>Displays MCL entries or best effort method (BEM)/Parser Return Code (PRC) failures.</td>
</tr>
<tr>
<td>bem</td>
<td>Displays a BEM failed command list, and forces the standby switch to reboot.</td>
</tr>
<tr>
<td>mcl</td>
<td>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.</td>
</tr>
<tr>
<td>prc</td>
<td>Displays a PRC failed command list and forces the standby switch to reboot.</td>
</tr>
<tr>
<td>ignored failures mcl</td>
<td>Displays the ignored MCL failures.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
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 stackwise-virtual

To display your Cisco StackWise Virtual configuration information, use the `show stackwise-virtual` command.

```
show stackwise-virtual { [switch [switch number <1-2>]] | (link | bandwidth | neighbors | dual-active-detection) }
```

**Syntax Description**

- **switch number** (Optional) Displays information of a particular switch in the stack.
- **link** Displays Stackwise Virtual link information.
- **bandwidth** Displays bandwidth availability for StackWise Virtual.
- **neighbors** Displays Stackwise Virtual neighbors.
- **dual-active-detection** Displays Stackwise-Virtual dual-active-detection information.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following is a sample output from the `show stackwise-virtual` command:

```
Device# show stackwise-virtual

Stackwise Virtual: <Enabled/Disabled>
Domain Number: <Domain Number>
Switch Stackwise Virtual Link Ports
--------- --------------------------- ---------------------------
1 1 Tengigabitethernet1/0/4
2 1 Tengigabitethernet1/0/5
2 2 Tengigabitethernet2/0/4
2 2 Tengigabitethernet2/0/5
```

The following is a sample output from the `show stackwise-virtual link` command:

```
Device# show stackwise-virtual link

Stackwise Virtual Link (SVL) Information:
------------------------------------------
Flags:
```
### Link Status

<table>
<thead>
<tr>
<th>Switch</th>
<th>SVL</th>
<th>Ports</th>
<th>Link-Status</th>
<th>Protocol-Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>FortyGigabitEthernet1/1/1</td>
<td>U</td>
<td>R</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>FortyGigabitEthernet2/1/1</td>
<td>U</td>
<td>R</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show stackwise-virtual bandwidth` command:

Device#`show stackwise-virtual bandwidth`

Switch Bandwidth

1  160
2  160

The following is a sample output from the `show stackwise-virtual neighbors` command:

Device#`show stackwise-virtual neighbors`

<table>
<thead>
<tr>
<th>Switch Number</th>
<th>Local Interface</th>
<th>Remote Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tengigabitethernet1/0/1</td>
<td>Tengigabitethernet2/0/1</td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet1/0/2</td>
<td>Tengigabitethernet2/0/2</td>
</tr>
<tr>
<td>2</td>
<td>Tengigabitethernet2/0/1</td>
<td>Tengigabitethernet1/0/1</td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet2/0/2</td>
<td>Tengigabitethernet2/0/2</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show stackwise-virtual dual-active-detection` command:

Device#`show stackwise-virtual dual-active-detection`

Stackwise Virtual Dual-Active-Detection (DAD) Configuration:

<table>
<thead>
<tr>
<th>Switch Number</th>
<th>Local Interface</th>
<th>Remote Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tengigabitethernet1/0/10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet1/0/11</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tengigabitethernet2/0/12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet2/0/13</td>
<td></td>
</tr>
</tbody>
</table>

Stackwise Virtual Dual-Active-Detection (DAD) Configuration After Reboot:

<table>
<thead>
<tr>
<th>Switch Number</th>
<th>Local Interface</th>
<th>Remote Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Tengigabitethernet1/0/10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet1/0/11</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Tengigabitethernet2/0/12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tengigabitethernet2/0/13</td>
<td></td>
</tr>
</tbody>
</table>
show tech-support stack

To display all switch stack-related information for use by technical support, use the `show tech-support stack` command in privileged EXEC mode.

**show tech-support stack**

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>The output for this command was enhanced to include more stack-related information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show tech-support stack` command captures the snapshot of stacking states and information for debug issues. Use this command, when stacking issues (such as stack cable issue, silent reload, switch not coming to ready state, stack crash, and so on) occur.

The output of the `show tech-support stack` command is very long. To better manage this output, you can redirect the output to a file (for example, `show tech-support stack | redirect flash:filename`) in the local writable storage file system or remote file system.

The output of the `show tech stack` command displays the output of the following commands:

The following commands are only available on stacked switches in ready state

- `show platform software stack-mgr switch`
- `show platform software sif switch`
- `show platform hardware fed switch`
- `dir crashinfo:`
- `dir flash:/core`

**Cisco Catalyst 9500 Series Switches with Stackwise Virtual Link**

- `show clock`
- `show version`
- `show running-config`

The following commands are only available on non-stackable switches in ready state:

- `show redundancy switchover history`
- `show platform software fed switch active`
- `show platform software fed switch standby`
- `show stackwise-virtual bandwidth`
- show stackwise-virtual dual-active-detection
- show stackwise-virtual link
- show stackwise-virtual neighbors
- dir crashinfo:
- dir flash:/core

The following is sample output from the `show tech-support stack` command:

```
Device# show tech-support stack
.
.
------------------ show stackwise-virtual bandwidth ------------------
Switch  Bandwidth
-------  ---------
 1       400G
 2       400G

------------------ show stackwise-virtual dual-active-detection ------------------
In dual-active recovery mode: No
Recovery Reload: Enabled
Dual-Active-Detection Configuration:
-------------------------------------
Switch  Dad port  Status
-------  ----------

------------------ show stackwise-virtual dual-active-detection pagp ------------------
Pagp dual-active detection enabled: No
In dual-active recovery mode: No
Recovery Reload: Enabled

No PAgP channel groups configured

------------------ show stackwise-virtual link ------------------
Stackwise Virtual Link(SVL) Information:
----------------------------------------
Flags:
------
Link Status
--------
U-Up D-Down
Protocol Status
----------
S-Suspended P-Pending E-Error T-Timeout R-Ready
-----------------------------------------------
Switch  SVL  Ports  Link-Status  Protocol-Status
-------  ---  ------  ---------        ---------
 1  1  HundredGigE1/0/45  D  R
 1  1  HundredGigE1/0/46  D  R
```
show tech-support stack

------------------ show stackwise-virtual link detail ------------------

------------------ show stackwise-virtual neighbors ------------------

Stackwise Virtual Link(SVL) Neighbors Information:
------------------------------------------------------------------
<table>
<thead>
<tr>
<th>Switch</th>
<th>SVL</th>
<th>Local Port</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>HundredGigE1/0/45</td>
<td>HundredGigE2/0/45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE1/0/46</td>
<td>HundredGigE2/0/46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE1/0/47</td>
<td>HundredGigE2/0/47</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE1/0/48</td>
<td>HundredGigE2/0/48</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>HundredGigE2/0/45</td>
<td>HundredGigE1/0/45</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE2/0/46</td>
<td>HundredGigE1/0/46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE2/0/47</td>
<td>HundredGigE1/0/47</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HundredGigE2/0/48</td>
<td>HundredGigE1/0/48</td>
</tr>
</tbody>
</table>

------------------ dir crashinfo-1: ------------------

------------------ dir flash-1:/core ------------------

------------------ dir crashinfo: ------------------

Directory of crashinfo:/

| 15778 -rw- 337 Dec 9 2018 09:29:47 +00:00 shutdown_fp0.log |
| 15779 -rw- 336 Dec 9 2018 09:29:48 +00:00 shutdown_cc1.log |
| 15780 -rw- 3675 Dec 9 2018 09:29:50 +00:00 shutdown_rp0.log |
| 15781 drwx 147456 Jun 27 2019 18:21:13 +00:00 tracelogs |
| 15910 drwx 8192 Jun 24 2019 08:58:06 +00:00 license_evlog |
| 16372 -rw- 6769749 Dec 10 2018 07:12:56 +00:00 |

COMMAND REFERENCE, CISCO IOS XE GIBRALTAR 16.12.x (CATALYST 9500 SWITCHES)
The output fields are self-explanatory.
**stackwise-virtual**

To enable Cisco StackWise Virtual on a switch, use the `stackwise-virtual` command in the global configuration mode. To disable Cisco StackWise Virtual, use the `no` form of this command.

```
stackwise-virtual
no stackwise-virtual
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>stackwise-virtual</code></td>
<td>Enables Cisco StackWise Virtual.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After disabling Cisco StackWise Virtual, the switches must be reloaded to unstack them.

**Example**

The following example shows how to enable Cisco StackWise Virtual:

```
Device(config)# stackwise-virtual
```
**stackwise-virtual dual-active-detection**

To configure an interface as dual-active-detection link, use the `stackwise-virtual dual-active-detection` command in the interface configuration mode. To disassociate the interface, use the `no` form of the command.

```
stackwise-virtual dual-active-detection
no stackwise-virtual dual-active-detection
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stackwise-virtual</td>
<td>dual-active-detection</td>
<td>Enables Cisco StackWise Virtual dual-active-detection for the specified 10-G or 40-G interface.</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.6.1</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to configure a 10 Gigabit Ethernet interface as Dual-Active-Detection link:

```
Device(config)# interface TenGigabitEthernet1/0/2
Device(config-if)# stackwise-virtual dual-active-detection
```
stackwise-virtual link

To associate an interface with configured StackWise Virtual link, use the **stackwise-virtual link** command in the interface configuration mode. To disassociate the interface, use the **no** form of the command.

```
stackwise-virtual link  link-value
no stackwise-virtual link  link-value
```

**Syntax Description**

- **stackwise-virtual link**
  Associates a 10-G or 40-G interface to StackWise Virtual link.

- **link value**
  Domain ID configured for Cisco StackWise Virtual.

**Command Default**

Disabled.

**Command Modes**

Interface configuration (config-if).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.6.1</td>
<td></td>
</tr>
</tbody>
</table>

**Example:**

This example shows how to associate a 40 Gigabit Ethernet interface with configured Stackwise Virtual Link (SVL):

```
Device(config)# interface FortyGigabitEthernet1/1/1
Device(config-if)# stackwise-virtual link 1
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)#
```
To put the system into maintenance mode, use the **start maintenance** command in the privileged EXEC mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>start maintenance</td>
<td>Puts the system into maintenance mode.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to start maintenance mode:

```
Device# start maintenance
```
stop maintenance

To put the system out of maintenance mode, use the **stop maintenance** command in the privileged EXEC mode.

**stop maintenance**

**Command Default**

Disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to stop maintenance mode:

```console
Device# stop maintenance
```
# system mode maintenance

To enter the system mode maintenance configuration mode, use the `system mode maintenance` command in the global configuration mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>system mode maintenance</code></td>
<td>Enters the maintenance configuration mode.</td>
</tr>
</tbody>
</table>

**Command Default**

Disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example:**

The following example shows how to enter the maintenance configuration mode:

```
Device(config)# system mode maintenance
Device(config-maintenance)#
```
PART III

Interface and Hardware Components

• Interface and Hardware Commands, on page 145
Interface and Hardware Commands

• bluetooth pin, on page 147
• debug ipower, on page 148
• debug interface, on page 149
• debug lldp packets, on page 150
• debug platform poe, on page 151
• debug platform software fed switch active punt packet-capture start, on page 152
• duplex, on page 153
• enable (interface configuration), on page 155
• errdisable detect cause, on page 156
• errdisable recovery cause, on page 158
• errdisable recovery cause, on page 160
• interface, on page 162
• interface range, on page 164
• ip mtu, on page 166
• ipv6 mtu, on page 167
• lldp (interface configuration), on page 168
• mode (power-stack configuration), on page 170
• network-policy, on page 172
• network-policy profile (global configuration), on page 173
• power-priority , on page 174
• power supply, on page 176
• shell trigger, on page 178
• show beacon all, on page 179
• show env, on page 180
• show errdisable detect, on page 183
• show errdisable recovery, on page 185
• show interfaces, on page 186
• show interfaces counters, on page 189
• show interfaces switchport, on page 191
• show interfaces transceiver, on page 193
• show inventory, on page 197
• show memory platform, on page 203
• show module, on page 206
• show mgmt-infra trace messages ilpower, on page 207
• show mgmt-infra trace messages ilpower-ha, on page 209
• show mgmt-infra trace messages platform-mgr-poe, on page 210
• show network-policy profile, on page 211
• show platform hardware bluetooth, on page 212
• show platform hardware capacity, on page 213
• show platform hardware fed switch forward, on page 225
• show platform hardware fed switch forward interface, on page 228
• show platform hardware fed switch forward last summary, on page 231
• show platform resources, on page 234
• show platform software audit, on page 235
• show platform software fed switch punt cpuq rates, on page 239
• show platform software fed switch punt packet-capture display, on page 241
• show platform software fed switch punt rates interfaces, on page 243
• show platform software ilpower, on page 246
• show platform software memory, on page 248
• show platform software process list, on page 253
• show platform software process memory, on page 257
• show platform software process slot switch, on page 260
• show platform software status control-processor, on page 262
• show platform software thread list, on page 265
• show processes cpu platform, on page 267
• show processes cpu platform history, on page 270
• show processes cpu platform monitor, on page 273
• show processes memory platform, on page 275
• show processes platform, on page 279
• show system mtu, on page 282
• show tech-support, on page 283
• show tech-support bgp, on page 285
• show tech-support diagnostic, on page 288
• show tech-support poe, on page 290
• speed, on page 305
• switchport block, on page 307
• system mtu, on page 308
• voice-signaling vlan (network-policy configuration), on page 309
• voice vlan (network-policy configuration), on page 311
**bluetooth pin**

To configure a new Bluetooth pin, use the `bluetooth pin` command in interface configuration or global configuration mode.

```
bluetooth pin pin
```

**Syntax Description**

- **pin**: Pairing pin for the Bluetooth interface.
  The pin is a 4-digit number.

**Command Modes**

- Interface configuration (config-if)
- Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `bluetooth pin` command can be configured either in the interface configuration or global configuration mode. Cisco recommends using the global configuration mode to configure the Bluetooth pin.

**Examples**

This example shows how to configure a new Bluetooth pin using the `bluetooth pin` command.

```
Device> enable
Device# configure terminal
Device(config)# bluetooth pin 1111
Device(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform hardware bluetooth</td>
<td>Displays information about the Bluetooth interface</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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. You also can use the **remote command stack-member-number LINE** EXEC command on the active switch to enable debugging on a member switch without first starting a session.
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.

```
dbg interface interface-id | counters exceptions | protocol memory | null interface-number | port-channel port-channel-number | states | vlan vlan-id
no dbg interface interface-id | counters exceptions | protocol memory | null interface-number | port-channel port-channel-number | states | vlan vlan-id
```

**Syntax Description**

- **interface-id**
  - ID of the physical interface. Displays debug messages for the specified physical port, identified by type switch number/module number/port, for example, gigabitethernet 1/0/2.

- **null interface-number**
  - Displays debug messages for null interfaces. The interface number is always 0.

- **port-channel port-channel-number**
  - Displays debug messages for the specified EtherChannel port-channel interface. The port-channel-number range is 1 to 48.

- **vlan vlan-id**
  - Displays debug messages for the specified VLAN. The vlan range is 1 to 4094.

- **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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. You also can use the **remote command** stack-member-number LINE EXEC command on the active switch to enable debugging on a member switch without first starting a session.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **undebug lldp packets** command is the same as the **no debug lldp packets** command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the **session switch-number** EXEC command.
debug 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error</td>
<td>(Optional) Displays PoE-related error debug messages.</td>
</tr>
<tr>
<td>info</td>
<td>(Optional) Displays PoE-related information debug messages.</td>
</tr>
<tr>
<td>switch switch-number</td>
<td>(Optional) Specifies the stack member. This keyword is supported only on stacking-capable switches.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undebug platform poe` command is the same as the `no debug platform poe` command.
debug platform software fed switch active punt packet-capture start

To enable debugging of packets during high CPU utilization, for an active switch, use the `debug platform software fed switch active punt packet-capture start` command in privileged EXEC mode. To disable debugging of packets during high CPU utilization, for an active switch, use the `debug platform software fed switch active punt packet-capture stop` command in privileged EXEC mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch active</code></td>
<td>Displays information about the active switch.</td>
</tr>
<tr>
<td><code>punt</code></td>
<td>Specifies the punt information.</td>
</tr>
<tr>
<td><code>packet-capture</code></td>
<td>Specifies information about the captured packet.</td>
</tr>
<tr>
<td><code>start</code></td>
<td>Enables debugging of the active switch.</td>
</tr>
<tr>
<td><code>stop</code></td>
<td>Disables debugging of the active switch.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `debug platform software fed switch active punt packet-capture start` command starts the debugging of packets during high CPU utilization. The packet capture is stopped when the 4k buffer size is exceeded.

**Examples**

The following is a sample output from the `debug platform software fed switch active punt packet-capture start` command:

```
Device# debug platform software fed switch active punt packet-capture start
Punt packet capturing started.
```

The following is a sample output from the `debug platform software fed switch active punt packet-capture stop` command:

```
Device# debug platform software fed switch active punt packet-capture stop
Punt packet capturing stopped. Captured 101 packet(s)
```
duplex

To specify the duplex mode of operation for a port, use the `duplex` command in interface configuration mode. To return to the default value, use the `no` form of this command.

```
duplex {auto | full | half}
no duplex {auto | full | half}
```

**Syntax Description**
- `auto`: Enables automatic duplex configuration. The port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode.
- `full`: Enables full-duplex mode.
- `half`: Enables half-duplex mode (only for interfaces operating at 10 or 100 Mb/s). You cannot configure half-duplex mode for interfaces operating at 1000 or 10,000 Mb/s.

**Command Default**
The default is `auto` for Gigabit Ethernet ports.

Duplex options are not supported on the 1000BASE-x or 10GBASE-x (where -x is -BX, -CWDM, -LX, -SX, or -ZX) small form-factor pluggable (SFP) modules.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
For Gigabit Ethernet ports, setting the port to `auto` has the same effect as specifying `full` if the attached device does not autonegotiate the duplex parameter.

**Note**
Half-duplex mode is supported on Gigabit Ethernet interfaces if the duplex mode is `auto` and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

Certain ports can be configured to be either full duplex or half duplex. How this command is applied depends on the device to which the switch is attached.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces, and use the `auto` setting on the supported side.

If the speed is set to `auto`, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to `auto`. 
Changing the interface speed and duplex mode configuration might shut down and reenable the interface during the reconfiguration.

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

**Examples**

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

```
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# duplex full
```
enable (interface configuration)

To enable the 100 GigabitEthernet interface, use the `enable` command in interface configuration mode. Use the `no` form of the command to disable a 100 GigabitEthernet interface.

```
enable

no enable
```

**Command Default**

The 100 GigabitEthernet interface is enabled on physical port numbers 25 through 32.

The 100 GigabitEthernet interface is disabled on physical port numbers 1 through 24.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>The command was introduced on the Cisco Catalyst 9500 Series Switches - High Performance.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `enable` command in the interface configuration mode, to enable the 100 GigabitEthernet interface.

Use the `no` version of the command to disable the 100 GigabitEthernet interface.

To display the current state of an interface, enter the `show interface interface-id` command in privileged EXEC mode.

The following example shows how to enable interface HundredGigabitEthernet 1/0/40.

When you enable the interface HundredGigabitEthernet 1/0/40, the corresponding 40 GigabitEthernet interfaces, FortyGigabitEthernet 1/0/15 and FortyGigabitEthernet 1/0/16 become inactive.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface hundredgigabitethernet 1/0/40
Device(config-if)# enable
```

The following example shows how to disable interface HundredGigabitEthernet 1/0/40 to use interface 40 GigabitEthernet 1/0/16.

When you disable a HundredGigabitEthernet interface, both the corresponding 40 GigabitEthernet interfaces, FortyGigabitEthernet1/015 and FortyGigabitEthernet1/0/16 become active.

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface hundredgigabitethernet 1/0/40
Device(config-if)# no enable
Device(config-if)# exit
```
**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 | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown vlan | 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 | link-flap | loopback | pagp-flap | pppoe-ia-rate-limit | psp shutdown vlan | security-violation shutdown vlan | sfp-config-mismatch}
```

**Syntax Description**

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

For protocol storm protection, excess packets are dropped for a maximum of two virtual ports. Virtual port error disabling using the `psp` keyword is not supported for EtherChannel and Flexlink interfaces.

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Enables the timer to recover from all error-disabled causes.</td>
</tr>
<tr>
<td>arp-inspection</td>
<td>Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.</td>
</tr>
<tr>
<td>bpduguard</td>
<td>Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.</td>
</tr>
<tr>
<td>channel-misconfig</td>
<td>Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.</td>
</tr>
<tr>
<td>dhcp-rate-limit</td>
<td>Enables the timer to recover from the DHCP snooping error-disabled state.</td>
</tr>
<tr>
<td>dtp-flap</td>
<td>Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.</td>
</tr>
</tbody>
</table>
| 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. |
<p>| 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. |</p>
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-mode-failure</td>
<td>Enables the timer to recover from the port mode change failure error-disabled state.</td>
</tr>
<tr>
<td>pppoe-ia-rate-limit</td>
<td>Enables the timer to recover from the PPPoE IA rate limit error-disabled state.</td>
</tr>
<tr>
<td>psecure-violation</td>
<td>Enables the timer to recover from a port security violation disable state.</td>
</tr>
<tr>
<td>psp</td>
<td>Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.</td>
</tr>
<tr>
<td>security-violation</td>
<td>Enables the timer to recover from an IEEE 802.1x-violation disabled state.</td>
</tr>
<tr>
<td>sfp-config-mismatch</td>
<td>Enables error detection on an SFP configuration mismatch.</td>
</tr>
<tr>
<td>storm-control</td>
<td>Enables the timer to recover from a storm control error.</td>
</tr>
<tr>
<td>udld</td>
<td>Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.</td>
</tr>
</tbody>
</table>

**Command Default**

Recovery is disabled for all causes.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A cause (such as all or BDPU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

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

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

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

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

**Examples**

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

```
Device# configure terminal
Device(config)# errdisable recovery cause bpdu-guard
```
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 | link-flap | loopback | mac-limit | pagp-flap | port-mode-failure | pppoe-ia-rate-limit | psecure-violation | psp | security-violation | sfp-config-mismatch | storm-control | udid}
```

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Enables the timer to recover from all error-disabled causes.</td>
</tr>
<tr>
<td><code>arp-inspection</code></td>
<td>Enables the timer to recover from the Address Resolution Protocol (ARP) inspection error-disabled state.</td>
</tr>
<tr>
<td><code>bpduguard</code></td>
<td>Enables the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state.</td>
</tr>
<tr>
<td><code>channel-misconfig</code></td>
<td>Enables the timer to recover from the EtherChannel misconfiguration error-disabled state.</td>
</tr>
<tr>
<td><code>dhcp-rate-limit</code></td>
<td>Enables the timer to recover from the DHCP snooping error-disabled state.</td>
</tr>
<tr>
<td><code>dtp-flap</code></td>
<td>Enables the timer to recover from the Dynamic Trunking Protocol (DTP) flap error-disabled state.</td>
</tr>
<tr>
<td><code>gbic-invalid</code></td>
<td>Enables the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disabled state.</td>
</tr>
</tbody>
</table>

**Note** This error refers to an invalid small form-factor pluggable (SFP) error-disabled state.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>inline-power</code></td>
<td>Enables the timer to recover from the Power over Ethernet (PoE) error-disabled state. This keyword is supported only on switches with PoE ports.</td>
</tr>
<tr>
<td><code>link-flap</code></td>
<td>Enables the timer to recover from the link-flap error-disabled state.</td>
</tr>
<tr>
<td><code>loopback</code></td>
<td>Enables the timer to recover from a loopback error-disabled state.</td>
</tr>
<tr>
<td><code>mac-limit</code></td>
<td>Enables the timer to recover from the mac limit error-disabled state.</td>
</tr>
<tr>
<td><code>pagp-flap</code></td>
<td>Enables the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state.</td>
</tr>
</tbody>
</table>
Enablesthetimertorecoverfromtheportmodechangefailure
error-disabledstate.

<table>
<thead>
<tr>
<th>port-mode-failure</th>
<th>Enables the timer to recover from the port mode change failure error-disabled state.</th>
</tr>
</thead>
</table>

Enables the timer to recover from the PPPoE IA rate limit error-disabled state.

<table>
<thead>
<tr>
<th>pppoe-ia-rate-limit</th>
<th>Supports PPPoE IA rate limit error-disabled state.</th>
</tr>
</thead>
</table>

Enables the timer to recover from a port security violation disable state.

<table>
<thead>
<tr>
<th>psecure-violation</th>
<th>Enables the timer to recover from a port security violation disable state.</th>
</tr>
</thead>
</table>

Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.

<table>
<thead>
<tr>
<th>psp</th>
<th>Enables the timer to recover from the protocol storm protection (PSP) error-disabled state.</th>
</tr>
</thead>
</table>

Enables the timer to recover from an IEEE 802.1x-violation disable state.

<table>
<thead>
<tr>
<th>security-violation</th>
<th>Enables the timer to recover from an IEEE 802.1x-violation disable state.</th>
</tr>
</thead>
</table>

Enables error detection on an SFP configuration mismatch.

<table>
<thead>
<tr>
<th>sfp-config-mismatch</th>
<th>Enables error detection on an SFP configuration mismatch.</th>
</tr>
</thead>
</table>

Enables the timer to recover from a storm control error.

<table>
<thead>
<tr>
<th>storm-control</th>
<th>Enables the timer to recover from a storm control error.</th>
</tr>
</thead>
</table>

Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.

<table>
<thead>
<tr>
<th>udld</th>
<th>Enables the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state.</th>
</tr>
</thead>
</table>

Recovery is disabled for all causes.

Command Default

| Recovery is disabled for all causes. |

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

A cause (such as all or BDPU guard) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in the error-disabled state, an operational state similar to link-down state.

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

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

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

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

Examples

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

```
Device# configure terminal
Device(config)# errdisable recovery cause bpdu-guard
```
interface

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

```
interface  
  | Auto-Template  interface-number  
  | FortyGigabitEthernet  
  | switch-number/slot-number/port-number  
  | GigabitEthernet  
  | switch-number/slot-number/port-number  
  | Group VI  
  | Group VI interface number  
  | Internal Interface  
  | Internal Interface number  
  | Loopback  
  | interface-number  
  | Null  
  | interface-number  
  | Port-channel  
  | interface-number  
  | TenGigabitEthernet  
  | switch-number/slot-number/port-number  
  | Tunnel  
  | interface-number  
  | Vlan  
  | interface-number  
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Template  interface-number</td>
<td>Enables you to configure a auto-template interface. The range is from 1 to 999.</td>
</tr>
</tbody>
</table>
| FortyGigabitEthernet  
  | switch-number/slot-number/port-number | Enables you to configure a 40-Gigabit Ethernet interface. |
|  
  |  
  | • switch-number — Switch ID. The range is from 1 to 8. |
|  
  |  
  | • slot-number — Slot number. Value is 1. |
|  
  |  
  | • port-number — Port number. The range is from 1 to 2. |
| GigabitEthernet  
  | switch-number/slot-number/port-number | Enables you to configure a Gigabit Ethernet IEEE 802.3z interface. |
|  
  |  
  | • switch-number — Switch ID. The range is from 1 to 8. |
|  
  |  
  | • slot-number — Slot number. The range is from 0 to 1. |
|  
  |  
  | • port-number — Port number. The range is from 1 to 48. |
| Group VI  
  | Group VI interface number | Enables you to configure a Group VI interface. The range is from 0 to 9. |
| Internal Interface  
  | Internal Interface | Enables you to configure an internal interface. |
| Loopback  
  | interface-number | Enables you to configure a loopback interface. The range is from 0 to 2147483647. |
| Null  
  | interface-number | Enables you to configure a null interface. The default value is 0. |
| Port-channel  
  | interface-number | Enables you to configure a port-channel interface. The range is from 1 to 128. |
**TenGigabitEthernet**  
*switch-number/slot-number/port-number*  
Enables you to configure a 10-Gigabit Ethernet interface.

- **switch-number** — Switch ID. The range is from 1 to 8.
- **slot-number** — Slot number. The range is from 0 to 1.
- **port-number** — Port number. The range is from 1 to 24 and 37 to 48.

**Tunnel**  
*interface-number*  
Enables you to configure a tunnel interface. The range is from 0 to 2147483647.

**Vlan**  
*interface-number*  
Enables you to configure a switch VLAN. The range is from 1 to 4094.

---

**Command Default**

None

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Examples**

The following example shows how to configure a tunnel interface:

```
Device(config)# interface Tunnel 15
Device(config-if)#
```

The following example shows how to configure a 40-Gigabit Ethernet interface:

```
Device(config)# interface FortyGigabitEthernet 1/1/2
Device(config-if)#
```
# interface range

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

```plaintext
interface range { Auto-Template interface-number | FortyGigabitEthernet switch-number/stack-number/port-number | GigabitEthernet switch-number/stack-number/port-number | Group VI Group VI interface number | Internal Interface Internal Interface number | Loopback interface-number Null interface-number Port-channel interface-number TenGigabitEthernet switch-number/stack-number/port-number Tunnel interface-number Vlan interface-number }
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Auto-Template</strong></td>
<td>Enables you to configure an auto-template interface. The range is from 1 to 999.</td>
</tr>
<tr>
<td><strong>FortyGigabitEthernet</strong></td>
<td>Enables you to configure a 40-Gigabit Ethernet interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>switch-number</code> — Switch ID. The range is from 1 to 8.</td>
</tr>
<tr>
<td></td>
<td>• <code>slot-number</code> — Slot number. Value is 1.</td>
</tr>
<tr>
<td></td>
<td>• <code>port-number</code> — Port number. The range is from 1 to 2.</td>
</tr>
<tr>
<td><strong>GigabitEthernet</strong></td>
<td>Enables you to configure a Gigabit Ethernet IEEE 802.3z interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>switch-number</code> — Switch ID. The range is from 1 to 8.</td>
</tr>
<tr>
<td></td>
<td>• <code>slot-number</code> — Slot number. The range is from 0 to 1.</td>
</tr>
<tr>
<td></td>
<td>• <code>port-number</code> — Port number. The range is from 1 to 48.</td>
</tr>
<tr>
<td><strong>Group VI</strong></td>
<td>Enables you to configure a Group VI interface. The range is from 0 to 9.</td>
</tr>
<tr>
<td><strong>Internal Interface</strong></td>
<td>Enables you to configure an internal interface.</td>
</tr>
<tr>
<td><strong>Loopback</strong></td>
<td>Enables you to configure a loopback interface. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td><strong>Null</strong></td>
<td>Enables you to configure a null interface. The default value is 0.</td>
</tr>
<tr>
<td><strong>Port-channel</strong></td>
<td>Enables you to configure a port-channel interface. The range is from 1 to 128.</td>
</tr>
</tbody>
</table>
**TenGigabitEthernet**  
*switch-number/slot-number/port-number*  
Enables you to configure a 10-Gigabit Ethernet interface.

- *switch-number*  — Switch ID. The range is from 1 to 8.
- *slot-number*  — Slot number. The range is from 0 to 1.
- *port-number*  — Port number. The range is from 1 to 24 and 37 to 48.

**Tunnel**  
*interface-number*  
Enables you to configure a tunnel interface. The range is from 0 to 2147483647.

**Vlan**  
*interface-number*  
Enables you to configure a switch VLAN. The range is from 1 to 4094.

---

**Command Default**  
None

**Command Modes**  
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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**

`bytes`  MTU size, in bytes. The range is from 68 up to the system MTU value (in bytes).

**Command Default**

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

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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>
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>med-tlv-select</th>
<th>Selects an LLDP Media Endpoint Discovery (MED) time-length-value (TLV) element to send.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tlv</td>
<td>String that identifies the TLV element. Valid values are the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• inventory-management — LLDP MED Inventory Management TLV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• location — LLDP MED Location TLV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• network-policy — LLDP MED Network Policy TLV.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• power-management — LLDP MED Power Management TLV.</td>
</tr>
<tr>
<td></td>
<td>receive</td>
<td>Enables the interface to receive LLDP transmissions.</td>
</tr>
<tr>
<td></td>
<td>tlv-select</td>
<td>Selects the LLDP TLVs to send.</td>
</tr>
<tr>
<td></td>
<td>power-management</td>
<td>Sends the LLDP Power Management TLV.</td>
</tr>
<tr>
<td></td>
<td>transmit</td>
<td>Enables LLDP transmission on the interface.</td>
</tr>
</tbody>
</table>

**Command Default**

LLDP is disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
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**

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

**Command Default**

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

**Command Modes**

Power-stack configuration (config-stackpower)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
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 (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

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

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

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

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

**Syntax Description**

- **profile-number**  Network-policy profile number. The range is 1 to 4294967295.

**Command Default**

No network-policy profiles are defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

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

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

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

This example shows how to create network-policy profile 60:

```
Device(config)# network-policy profile 60
Device(config-network-policy)#
```
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}
o  no  power-priority {high | low | switch}
```

**Syntax Description**

- `high value` Sets the power priority for the ports configured as high-priority ports. The range is 1 to 27, with 1 as the highest priority. The `high` value must be lower than the value set for the low-priority ports and higher than the value set for the switch.

- `low value` Sets the power priority for the ports configured as low-priority ports. The range is 1 to 27. The `low` value must be higher than the value set for the high-priority ports and the value set for the switch.

- `switch value` Sets the power priority for the switch. The range is 1 to 27. The `switch` value must be lower than the values set for the low and high-priority ports.

**Command Default**

If no values are configured, the power stack randomly determines a default priority.

The default ranges are 1 to 9 for switches, 10 to 18 for high-priority ports, 19 to 27 for low-priority ports.

On non-PoE switches, the high and low values (for port priority) have no effect.

**Command Modes**

Switch stack-power configuration (config-stack)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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

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

**Syntax Description**

- `stack-member-number` Stack member number for which to configure the internal power supplies. The range is 1 to 9, depending on the number of switches in the stack.
  
  This parameter is available only on stacking-capable switches.

- `slot` Selects the switch power supply to set.

- `A` Selects the power supply in slot A.

- `B` Selects the power supply in slot B.

  **Note** Power supply slot B is the closest slot to the outer edge of the switch.

- `off` Sets the switch power supply to off.

- `on` Sets the switch power supply to on.

**Command Default**

The switch power supply is on.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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  DCB170SB05B  OK  Good  Good  250/390
  1B  Not Present
```
shell trigger

To create an event trigger, use the shell trigger command in global configuration mode. Use the no form of this command to delete the trigger.

`shell trigger identifier description`

`no shell trigger identifier description`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>identifier</code></td>
<td>Specifies the event trigger identifier. The identifier should have no spaces or hyphens between words.</td>
</tr>
<tr>
<td><code>description</code></td>
<td>Specifies the event trigger description text.</td>
</tr>
</tbody>
</table>

**Command Default**

System-defined event triggers:

- CISCO_DMP_EVENT
- CISCO_IPVSC_AUTO_EVENT
- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to create user-defined event triggers for use with the macro auto device and the macro auto execute commands.

To support dynamic device discovery when using IEEE 802.1x authentication, you need to configure the RADIUS authentication server to support the Cisco attribute-value pair: `auto-smart-port=event trigger`.

**Example**

This example shows how to create a user-defined event trigger called RADIUS_MAB_EVENT:

```
Device(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
Device(config)# end
```
show beacon all

To display the status of beacon LED on the device, use the `show beacon all` command in privileged EXEC mode.

```
show beacon { rp { active | standby } | slot slot-number } | all }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`rp (active</td>
<td>standby)`</td>
</tr>
<tr>
<td><code>slot slot-num</code></td>
<td>Specifies the slot whose beacon LED status is to be displayed.</td>
</tr>
<tr>
<td>all</td>
<td>Displays the status of all beacon LEDs.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Default**

This command has no default settings.

**Command Modes**

Privileged EXEC (#)

**Usage Guidelines**

Use the command `show beacon all` to know the status of all beacon LEDs.

**Sample output of show beacon all command.**

```
Device#show beacon all
Switch# Beacon Status
-----------------------
*1 OFF
```

**Sample output of show beacon rp command.**

```
Device#show beacon rp active
Switch# Beacon Status
-----------------------
*1 OFF
```

```
Device#show beacon slot 1
Switch# Beacon Status
-----------------------
*1 OFF
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Displays the fan and temperature environmental status and the status of the internal power supplies.</td>
</tr>
<tr>
<td><code>fan</code></td>
<td>Displays the switch fan status.</td>
</tr>
<tr>
<td><code>power</code></td>
<td>Displays the internal power status of the active switch.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>switch</code></td>
<td>(Optional) Displays the status of the internal power supplies for each switch in the stack or for the specified switch.</td>
</tr>
<tr>
<td><code>stack-member-number</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>stack</code></td>
<td>Displays all environmental status for each switch in the stack or for the specified switch.</td>
</tr>
<tr>
<td><code>temperature</code></td>
<td>Displays the switch temperature status.</td>
</tr>
<tr>
<td><code>status</code></td>
<td>(Optional) Displays the switch internal temperature (not the external temperature) and the threshold values.</td>
</tr>
</tbody>
</table>

**Command Default**
None

**Command Modes**
User EXEC (`->`)
Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
Inlet Temperature Value: 25 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius
Hotspot Temperature Value: 35 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius
SW PID Serial# Status Sys Pwr PoE Pwr Watts
-- ------------------ ---------- --------------- ------- ------- -----
1A Unknown Unknown No Input Power Bad    Bad 235
1B PWR-C1-350WAC DCB2137H04P OK Good    Good 350
```

```
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 Unknown Unknown No Input Power Bad    Bad 235
1B PWR-C1-350WAC DCB2137H04P OK Good    Good 350
```

```
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
Inlet Temperature Value: 25 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius
Hotspot Temperature Value: 35 Degree Celsius
```
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

This example shows how to display the temperature value, state, and the threshold values on a stack.

```
# show env stack
System Temperature Value: 41 Degree Celsius
System Temperature State: GREEN
Yellow Threshold : 66 Degree Celsius
Red Threshold : 76 Degree Celsius
```

This example shows the output of `show env temperature` command

```
Device> show env temperature
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 25 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 35 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius
```

**Table 7: States in the show env temperature status Command Output**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The switch temperature is in the <em>normal</em> operating range.</td>
</tr>
<tr>
<td>Yellow</td>
<td>The temperature is in the <em>warning</em> range. You should check the external temperature around the switch.</td>
</tr>
<tr>
<td>Red</td>
<td>The temperature is in the <em>critical</em> range. The switch might not run properly if the temperature is in this range.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

The error-disable reasons in the command output are listed in alphabetical order. The mode column shows how error-disable is configured for each feature.

You can configure error-disabled detection in these modes:

- `port mode`—The entire physical port is error-disabled if a violation occurs.
- `vlan mode`—The VLAN is error-disabled if a violation occurs.
- `port/vlan mode`—The entire physical port is error-disabled on some ports and is per-VLAN error-disabled on other ports.

This is an example of output from the `show errdisable detect` command:

```
Device> show errdisable detect
ErrDisable Reason       Detection Mode
----------------------------------------
arp-inspection          Enabled    port
bdpduguard              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-violation     Enabled    port
sfp-config-mismatch     Enabled    port
storm-control          Enabled    port
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Status</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>show errdisable detect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>udld</td>
<td>Enabled</td>
<td>port</td>
</tr>
<tr>
<td>vmps</td>
<td>Enabled</td>
<td>port</td>
</tr>
</tbody>
</table>
**show errdisable recovery**

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

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Everest 16.5.1a | 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.
# show interfaces

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

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

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-id</td>
<td>(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.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(Optional) VLAN identification. The range is 1 to 4094.</td>
</tr>
<tr>
<td>accounting</td>
<td>(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.</td>
</tr>
<tr>
<td>capabilities</td>
<td>(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.</td>
</tr>
<tr>
<td>module number</td>
<td>(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.</td>
</tr>
<tr>
<td>description</td>
<td>(Optional) Displays the administrative status and description set for an interface.</td>
</tr>
<tr>
<td>etherchannel</td>
<td>(Optional) Displays interface EtherChannel information.</td>
</tr>
<tr>
<td>flowcontrol</td>
<td>(Optional) Displays interface flow control information.</td>
</tr>
<tr>
<td>private-vlan mapping</td>
<td>(Optional) Displays private-VLAN mapping information for the VLAN switch virtual interfaces (SVIs). This keyword is not available if the switch is running the LAN base feature set.</td>
</tr>
<tr>
<td>pruning</td>
<td>(Optional) Displays trunk VTP pruning information for the interface.</td>
</tr>
<tr>
<td>stats</td>
<td>(Optional) Displays the input and output packets by switching the path for the interface.</td>
</tr>
</tbody>
</table>
(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**, **rate-limit**, and **shape** keywords are not supported.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

Note

The field **Last Input** displayed in the command output indicates the number of hours, minutes, and seconds since the last packet was successfully received by an interface and processed by the CPU on the device. This information can be used to know when a dead interface failed.

**Last Input** is not updated by fast-switched traffic.

The field **output** displayed in the command output indicates the number of hours, minutes, and seconds since the last packet was successfully transmitted by the interface. The information provided by this field can be useful for knowing when a dead interface failed.

```
Device# show interfaces accounting
Vlan1
  Protocol  Pkts In   Chars In  Pkts Out  Chars Out
  IP        0          0        6          378
Vlan200
  Protocol  Pkts In   Chars In  Pkts Out  Chars Out
```
No traffic sent or received on this interface.

**GigabitEthernet0/0**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Pkts In</th>
<th>Chars In</th>
<th>Pkts Out</th>
<th>Chars Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>165476</td>
<td>11417844</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Spanning</td>
<td>1240284</td>
<td>64494768</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CDP</td>
<td>7096</td>
<td>425760</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td>41368</td>
<td>18781072</td>
<td>82908</td>
<td>35318808</td>
</tr>
</tbody>
</table>

**GigabitEthernet1/0/1**

No traffic sent or received on this interface.

**GigabitEthernet1/0/2**

No traffic sent or received on this interface.

<output truncated>

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 fortyGigabitEthernet6/0/2 description
Interface Status Protocol Description
Fo1/0/2 up Connects to Marketing
```

```
Device# show interfaces etherchannel

Port-channel34:
Age of the Port-channel = 28d:18h:51m:46s
Logical slot/port = 12/34 Number of ports = 0
GC = 0x00000000 HotStandBy port = null
Passive port list =
Port state = Port-channel L3-Ag Ag-Not-Inuse
Protocol =
Port security = Disabled
```

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

```
Device# show interfaces status err-disabled
Port Name Status Reason
Fo1/0/2 err-disabled gbic-invalid
Fo2/0/3 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
```
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 member-number | protocol status | trunk} ]
```

**Syntax Description**

- **interface-id** (Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
- **errors** (Optional) Displays error counters.
- **etherchannel** (Optional) Displays EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent.
- **module member-number** (Optional) Displays counters for the specified member.
- **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 module 2. It displays all counters for the specified switch in the module.
Device# `show interfaces counters module 2`

<table>
<thead>
<tr>
<th>Port</th>
<th>InOctets</th>
<th>InUcastPkts</th>
<th>InMcastPkts</th>
<th>InBcastPkts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>520</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>520</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>520</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>520</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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

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`

<table>
<thead>
<tr>
<th>Port</th>
<th>TrunkFramesTx</th>
<th>TrunkFramesRx</th>
<th>WrongEncap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>80678</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>82320</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<output truncated>
show interfaces switchport

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

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

**Syntax Description**

- `interface-id` (Optional) ID of the interface. Valid interfaces include physical ports (including type, stack member for stacking-capable switches, module, and port number) and port channels. The port channel range is 1 to 48.

- `module number` (Optional) Displays switchport configuration of all interfaces on the switch or specified stack member. The range is 1 to 9. This option is not available if you entered a specific interface ID.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```
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

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

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

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

**Syntax Description**

- **interface-id** (Optional) ID of the physical interface, including type, stack member (stacking-capable switches only) module, and port number.
- **detail** (Optional) Displays calibration properties, including high and low numbers and any alarm information for any Digital Optical Monitoring (DoM)-capable transceiver if one is installed in the switch.
- **module number** (Optional) Limits display to interfaces on module on the switch. 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

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

```
Device# show interfaces transceiver

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Temperature (Celsius)</th>
<th>Voltage (Volts)</th>
<th>Current (mA)</th>
<th>Optical Tx Power (dBm)</th>
<th>Optical Rx Power (dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi5/1/2</td>
<td>42.9</td>
<td>3.28</td>
<td>22.1</td>
<td>-5.4</td>
<td>-8.1</td>
</tr>
<tr>
<td>Te5/1/3</td>
<td>32.0</td>
<td>3.28</td>
<td>19.8</td>
<td>2.4</td>
<td>-4.2</td>
</tr>
</tbody>
</table>
```

```
Device# show interfaces gigabitethernet1/1/1 transceiver properties
Name: Gi1/1/1
Administrative Speed: auto
```
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.

<table>
<thead>
<tr>
<th>Port</th>
<th>Temperature (Celsius)</th>
<th>High Alarm Threshold (Celsius)</th>
<th>High Warn Threshold (Celsius)</th>
<th>Low Warn Threshold (Celsius)</th>
<th>Low Alarm Threshold (Celsius)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/1/1</td>
<td>29.9</td>
<td>74.0</td>
<td>70.0</td>
<td>0.0</td>
<td>-4.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High Alarm Threshold (Volts)</td>
<td>High Warn Threshold (Volts)</td>
<td>Low Warn Threshold (Volts)</td>
<td>Low Alarm Threshold (Volts)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltage (Motls)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/1/1</td>
<td>3.28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optical Transmit Power (dBm)</td>
<td>High Alarm Threshold (dBm)</td>
<td>High Warn Threshold (dBm)</td>
<td>Low Warn Threshold (dBm)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gi1/1/1</td>
<td>1.8</td>
<td>7.9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optical Receive Power (dBm)</td>
<td>High Alarm Threshold (dBm)</td>
<td>High Warn Threshold (dBm)</td>
<td>Low Warn Threshold (dBm)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Gi1/1/1</td>
<td>1.8</td>
<td>7.9</td>
</tr>
</tbody>
</table>
```

```
Device# show interfaces transceiver supported-list
Transceiver Type     Cisco p/n min version supporting DOM
----------------------------------------------
DWDM GBIC            ALL
DWDM SFP             ALL
RX only WDM GBIC     ALL
DWDM XENPAK          ALL
DWDM X2              ALL
DWDM XFP             ALL
CWDM GBIC            NONE
CWDM X2              ALL
CWDM XFP             ALL
XENPAK ZR            ALL
X2 ZR                ALL
XFP ZR                ALL
Rx only WDM XENPAK   ALL
XENPAK_ER            10-1888-04
X2 ER                ALL
XFP_EER               ALL
XENPAK_LR            10-1838-04
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
This is an example of output from the `show interfaces transceiver threshold-table` command:

```
Device# show interfaces transceiver threshold-table

Optical Tx  Optical Rx  Temp  Laser Bias  Voltage
-----------  ----------  -----  ------------  --------
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
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show interfaces transceiver

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transceiver type all</td>
<td>Enters the transceiver type configuration mode.</td>
</tr>
<tr>
<td>monitoring</td>
<td>Enables digital optical monitoring.</td>
</tr>
</tbody>
</table>
show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the `show inventory` command in user EXEC or privileged EXEC mode.

`show inventory {fru | oid | raw} [entity]`

- **fru** (Optional) Retrieves information about all Field Replaceable Units (FRUs) installed in the Cisco networking device.
- **oid** (Optional) Retrieves information about the vendor specific hardware registration identifier referred to as object identifier (OID).
  The OID identifies the MIB object’s location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices.
- **raw** (Optional) Retrieves information about all Cisco products referred to as entities installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification.
- **entity** (Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display very specific UDI information; for example “sfslot 1” will display the UDI information for slot 1 of an entity named sfslot.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.3</td>
<td>This command was enhanced to display the serial number for the chassis.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show inventory` command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have subentities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.
Use the `show inventory` command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

The following is sample output from the `show inventory` command:

```
Device#show inventory
9500-32QC-SVL#show inv
NAME: "Switch 1 Chassis", DESCR: "Cisco Catalyst 9500 Series Chassis"
PID: C9500-32QC , VID: V00 , SN: CAT2144L10V

NAME: "Switch 1 Power Supply Module 0", DESCR: "Cisco Catalyst 9500 Series 650W AC Power Supply"

PID: C9K-PWR-650WAC-R , VID: V01 , SN: ART2151FC04

NAME: "Switch 1 Fan Tray 0", DESCR: "Cisco Catalyst 9500 Series Fan Tray"
PID: C9K-T1-FANTRAY , VID: , SN:

NAME: "Switch 1 Fan Tray 1", DESCR: "Cisco Catalyst 9500 Series Fan Tray"
PID: C9K-T1-FANTRAY , VID: , SN:

NAME: "Switch 1 Slot 1 Supervisor", DESCR: "Cisco Catalyst 9500 Series Router"
PID: C9500-32QC , VID: V00 , SN: CAT2144L10V

NAME: "FortyGigabitEthernet1/0/2", DESCR: "QSFP 40GE CU3M"
PID: QSFP-H40G-CU3M , VID: A0 , SN: JFC2144034J-A

NAME: "FortyGigabitEthernet1/0/4", DESCR: "QSFP 40GE SR4"
PID: QSFP-40G-SR4 , VID: 03 , SN: AVF182450YQ

NAME: "FortyGigabitEthernet1/0/5", DESCR: "QSFP 40GE AOC3M"
PID: QSFP-H40G-AOC3M , VID: D , SN: FIW211101UL-B

NAME: "FortyGigabitEthernet1/0/8", DESCR: "QSFP 40GE AOC3M"
PID: QSFP-H40G-AOC3M , VID: D , SN: FIW211101IN6-B

NAME: "FortyGigabitEthernet1/0/10", DESCR: "QSFP 40GE AOC3M"

NAME: "FortyGigabitEthernet1/0/11", DESCR: "QSFP 40GE CU3M"

NAME: "FortyGigabitEthernet1/0/15", DESCR: "QSFP 40GE AOC3M"
PID: QSFP-H40G-AOC3M , VID: D , SN: FIS1922011T-B

NAME: "FortyGigabitEthernet1/0/16-qsa", DESCR: "CVR 10GE SFP "
PID: CVR-QSFP-SFP10G , VID: V01 , SN: DTY2046040UN

NAME: "FortyGigabitEthernet1/0/16", DESCR: "10GE CU3M"

NAME: "FortyGigabitEthernet1/0/18", DESCR: "QSFP 40GE CU3M"
PID: QSFP-H40G-CU3M , VID: D , SN: TED2047K100-A

NAME: "FortyGigabitEthernet1/0/19", DESCR: "QSFP 40GE CU3M"
PID: QSFP-H40G-CU3M , VID: D , SN: TED2030K4U6-B

NAME: "FortyGigabitEthernet1/0/22", DESCR: "QSFP 40GE CU5M"
PID: QSFP-H40G-CU5M , VID: A0 , SN: JFC203508YN-B

NAME: "FortyGigabitEthernet1/0/24", DESCR: "QSFP 40GE CU3M"
```
show inventory

PID: QSFP-H40G-CU3M , VID: D , SN: TED2047K13Y-A
NAME: "FortyGigabitEthernet1/0/25", DESCR: "QSFP 100GE CU3M"

PID: QSFP-100G-CU3M , VID: A , SN: APF20412069-A
NAME: "FortyGigabitEthernet1/0/28", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: A0 , SN: JPC214402J7-A
NAME: "FortyGigabitEthernet1/0/30", DESCR: "QSFP 40GE CU3M"

NAME: "FortyGigabitEthernet1/0/32", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: 01 , SN: LCC1922G2E8-A
NAME: "FortyGigabitEthernet1/0/33", DESCR: "QSFP 100GE CU3M"

PID: QSFP-100G-CU3M , VID: A , SN: APF20412159-A
NAME: "FortyGigabitEthernet1/0/47", DESCR: "QSFP 40GE CU3M"

PID: QSFP-100G-CU3M , VID: A , SN: APF21010360-B
NAME: "FortyGigabitEthernet1/0/48", DESCR: "QSFP 100GE CU1M"

PID: C9500-32QC , VID: V00 , SN: CAT2144L10L
NAME: "Switch 2 Chassis", DESCR: "Cisco Catalyst 9500 Series Chassis"

PID: C9K-PWR-650WAC-R , VID: V00 , SN: ART2141FAZ4
NAME: "Switch 2 Power Supply Module 0", DESCR: "Cisco Catalyst 9500 Series 650W AC Power Supply"

PID: C9K-T1-FANTRAY , VID: , SN: 
NAME: "Switch 2 Fan Tray 4", DESCR: "Cisco Catalyst 9500 Series Fan Tray"
NAME: "Switch 2 Fan Tray 5", DESCR: "Cisco Catalyst 9500 Series Fan Tray"

PID: C9K-T1-FANTRAY , VID: , SN: 
NAME: "Switch 2 Slot 1 Supervisor", DESCR: "Cisco Catalyst 9500 Series Router"

PID: C9500-32QC , VID: V00 , SN: CAT2144L10L
NAME: "SATA disk", DESCR: "disk0 Drive"

PID: C9K-F1-SSD-240G , VID: V00 , SN: CAT2144L10J0
NAME: "FortyGigabitEthernet2/0/4", DESCR: "QSFP 40GE SR4"

PID: QSFP-40G-SR4 , VID: 03 , SN: AVP1824S0YS
NAME: "FortyGigabitEthernet2/0/6", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: D , SN: TED2047K0ZN-B
NAME: "FortyGigabitEthernet2/0/7", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: D , SN: TED2047K0ZN-A
NAME: "FortyGigabitEthernet2/0/8", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: D , SN: TED2030K4U6-A
NAME: "FortyGigabitEthernet2/0/9", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M , VID: A0 , SN: JPC2144034J-B
NAME: "FortyGigabitEthernet2/0/10", DESCR: "QSFP 40GE AOC10M"

NAME: "FortyGigabitEthernet2/0/11", DESCR: "QSFP 40GE CU5M"

PID: QSFP-H40G-CU5M , VID: A0 , SN: JPC203508R1-B
NAME: "FortyGigabitEthernet2/0/13", DESCR: "QSFP 40GE CU3M"
NAME: "FortyGigabitEthernet2/0/14", DESCR: "QSFP 40GE CU2M"

PID: QSFP-H40G-CU2M, VID: A0, SN: JFC2039000Z-A
NAME: "FortyGigabitEthernet2/0/15", DESCR: "QSFP 40GE AOC3M"

NAME: "FortyGigabitEthernet2/0/17", DESCR: "QSFP 40GE AOC3M"

PID: QSFP-H40G-AOC3M, VID: D, SN: FIW211101IN6-A
NAME: "FortyGigabitEthernet2/0/18", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-AOC3M, VID: D, SN: FIW211101UL-A
NAME: "FortyGigabitEthernet2/0/20", DESCR: "QSFP 40GE AOC3M"

PID: QSFP-H40G-AOC3M, VID: D, SN: FIS1922011T-A
NAME: "FortyGigabitEthernet2/0/21-qsa", DESCR: "CVR 10GE SFP"

PID: CVR-QSFP-SFP10G, VID: V01, SN: DTY20460528
NAME: "FortyGigabitEthernet2/0/21", DESCR: "10GE CU3M"

NAME: "FortyGigabitEthernet2/0/28", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M, VID: A0, SN: JPC214402J7-B
NAME: "FortyGigabitEthernet2/0/30", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M, VID: D, SN: TED2047K13Z-A
NAME: "FortyGigabitEthernet2/0/32", DESCR: "QSFP 40GE CU3M"

PID: QSFP-H40G-CU3M, VID: 01, SN: LCC1922G2EB-B
NAME: "HundredGigE2/0/33", DESCR: "QSFP 100GE CU3M"

PID: QSFP+100G-CU3M, VID: A, SN: APF21010653-B
NAME: "HundredGigE2/0/47", DESCR: "QSFP 100GE CU3M"

PID: QSFP+100G-CU3M, VID: A, SN: APF21010360-A
NAME: "HundredGigE2/0/48", DESCR: "QSFP 100GE CU1M"

PID: QSFP+100G-CU1M, VID: A, SN: APF21450009-B
NAME: "HundredGigE2/0/48", DESCR: "QSFP 100GE CU1M"

Table 8: show inventory Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME</td>
<td>Physical name (text string) assigned to the Cisco entity. For example, console or a simple component number (port or module number), such as “1,” depending on the physical component naming syntax of the device.</td>
</tr>
<tr>
<td>DESCR</td>
<td>Physical description of the Cisco entity that characterizes the object. The physical description includes the hardware serial number and the hardware revision.</td>
</tr>
<tr>
<td>PID</td>
<td>Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>VID</td>
<td>Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.</td>
</tr>
<tr>
<td>SN</td>
<td>Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.</td>
</tr>
</tbody>
</table>
For diagnostic purposes, the `show inventory` command can be used with the `raw` keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

The `raw` keyword option is primarily intended for troubleshooting problems with the `show inventory` command itself.

Enter the `show inventory` command with an `entity` argument value to display the UDI information for a specific type of Cisco entity installed in the networking device. In this example, a list of Cisco entities that match the sfslot argument string is displayed.

```
Device#show inventory "Switch 1 Chassis"
NAME: "Switch 1 Chassis", DESCR: "Cisco Catalyst 9500 Series Chassis"
   PID: C9500-32QC  , VID: V00  , SN: CAT2144L10V

NAME: "Switch 1 Power Supply Module 0", DESCR: "Cisco Catalyst 9500 Series 650W AC Power Supply"
   PID: C9K-PWR-650WAC-R  , VID: V00  , SN: ART2148FS3T

   PID: C9K-PWR-650WAC-R  , VID: V01  , SN: ART2151FC04

NAME: "Switch 1 Fan Tray 0", DESCR: "Cisco Catalyst 9500 Series Fan Tray"
   PID: C9K-T1-FANTRAY  , VID:  , SN:

NAME: "Switch 1 Fan Tray 1", DESCR: "Cisco Catalyst 9500 Series Fan Tray"
   PID: C9K-T1-FANTRAY  , VID:  , SN:

NAME: "Switch 1 Slot 1 Supervisor", DESCR: "Cisco Catalyst 9500 Series Router"
   PID: C9500-32QC  , VID: V00  , SN: CAT2144L10V

NAME: "FortyGigabitEthernet1/0/2", DESCR: "QSFP 40GE CU3M"
   PID: QSFP-H40G-CU3M  , VID: A0  , SN: JPC2144034J-A

NAME: "FortyGigabitEthernet1/0/4", DESCR: "QSFP 40GE SR4"
   PID: QSFP-40G-SR4  , VID: 03  , SN: AVP1824S0YQ

NAME: "FortyGigabitEthernet1/0/5", DESCR: "QSFP 40GE AOC3M"
   PID: QSFP-H40G-AOC3M  , VID: D  , SN: FW211101UL-B

NAME: "FortyGigabitEthernet1/0/6", DESCR: "QSFP 40GE AOC3M"
   PID: QSFP-H40G-AOC3M  , VID: D  , SN: FW211101NH-B

NAME: "FortyGigabitEthernet1/0/10", DESCR: "QSFP 40GE AOC3M"

NAME: "FortyGigabitEthernet1/0/11", DESCR: "QSFP 40GE CU3M"

NAME: "FortyGigabitEthernet1/0/15", DESCR: "QSFP 40GE AOC3M"
   PID: QSFP-H40G-AOC3M  , VID: D  , SN: FIS1922011T-B

NAME: "FortyGigabitEthernet1/0/16-qsa", DESCR: "CVR 10GE SFP"
   PID: CVR-QSFP-SFP10G  , VID: V01  , SN: DT20146040

NAME: "FortyGigabitEthernet1/0/16", DESCR: "10GE CU3M"

NAME: "FortyGigabitEthernet1/0/18", DESCR: "QSFP 40GE CU3M"
   PID: QSFP-H40G-CU3M  , VID: D  , SN: TED2047K100-A
```
You can request even more specific UDI information with the entity argument value enclosed in quotation marks.
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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
Mapped : 516316
NFS Unstable : 0
Page Tables : 17124
Slab : 0
```
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) : 437136

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

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

**Syntax Description**

- `switch-num` (Optional) Number of the switch.

**Command Default**

None

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Entering the `show module` command without the `switch-num` argument is the same as entering the `show module all` command.

The following example displays information for all modules on a Cisco Catalyst 9300 Series Switch:

```
Device# show module
Switch Ports Model Serial No. MAC address Hw Ver. Sw Ver.
------- ----- --------- ----------- -------------- ------- --------
1 40 C9300-24T FOC2147Q02D b4a8.b9c1.4100 V01 16.10.1
```
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.

**Syntax Description**

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch stack-member-number</td>
<td>(Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 for slot 1.
[10/23/12 14:05:10.984 UTC 2 3] Initialized inline power system configuration for slot 2.
[10/23/12 14:05:10.984 UTC 3 3] Initialized inline power system configuration for slot 3.
[10/23/12 14:05:10.984 UTC 5 3] Initialized inline power system configuration for slot 5.
[10/23/12 14:05:10.984 UTC 7 3] Initialized inline power system configuration for slot 7.
[10/23/12 14:05:10.984 UTC 8 3] Initialized inline power system configuration for slot 8.
[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 14:05:20.380 UTC 17 3] Gi1/0/24 port config Initialized
```
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 stack-member-number** (Optional) Specifies the stack member number for which to display inline power messages within a trace buffer.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This is an output example from the `show mgmt-infra trace messages ilpower-ha` command:

```
Device# show mgmt-infra trace messages ilpower-ha
```
**show mgmt-infra trace messages platform-mgr-poe**

To display platform manager Power over Ethernet (PoE) messages within a trace buffer, use the `show mgmt-infra trace messages platform-mgr-poe` privileged EXEC command.

```
show mgmt-infra trace messages platform-mgr-poe [switch stack-member-number]
```

**Syntax Description**

- `switch stack-member-number` (Optional) Specifies the stack member number for which to display messages within a trace buffer.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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] [detail]
```

**Syntax Description**

- `profile-number` (Optional) Displays the network-policy profile number. If no profile is entered, all network-policy profiles appear.
- `detail` (Optional) Displays detailed status and statistics information.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show network-policy profile` command:

```
Device# show network-policy profile
Network Policy Profile 10
  voice vlan 17 cos 4
  Interface:
    none
Network Policy Profile 30
  voice vlan 30 cos 5
  Interface:
    none
Network Policy Profile 36
  voice vlan 4 cos 3
  Interface:
    Interface_id
```
show platform hardware bluetooth

To display information about Bluetooth interface, use the `show platform hardware bluetooth` command in privileged EXEC mode.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show platform hardware bluetooth` command is to be used when an external USB Bluetooth dongle is connected on the device.

**Examples**

This example shows how to display the information of the Bluetooth interface using the `show platform hardware bluetooth` command.

```
Device> enable
Device# show platform hardware bluetooth
Controller: 0:1a:7d:da:71:13
Type: Primary
Bus: USB
State: DOWN
Name:
HCI Version:
```
show platform hardware capacity

This command is not supported on the C9500-12Q-E, C9500-12Q-A, C9500-24Q-E, C9500-24Q-A, C9500-40X-E, and C9500-40X-A models of the Cisco Catalyst 9500 Series Switches.

To determine system hardware capacity, use the show platform hardware capacity command in privileged EXEC mode.

show platform hardware capacity

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Example

This example shows how to determine the system hardware capacity

```
Device# show platform hardware capacity

Module       Model            Operational Status
------------- -------------------- ------------------------
subslot 1/0   C9500H-32QC      ok

Load Average
Slot Status  1-Min  5-Min  15-Min
RP0 Healthy  0.07    0.16    0.13

Memory (kB)
Slot Status   Total     Used (Pct) Free (Pct) Committed (Pct)
RP0 Healthy   15958108 3060492 (19%) 12897616 (81%) 25941080 (163%)  

CPU Utilization
Slot  CPU  User  System  Nice  Idle  IRQ  SIRQ  IOwait
RP0  0.70  0.20  0.00  99.10  0.00  0.00  0.00
1  0.39  0.09  0.00  99.50  0.00  0.00  0.00
2  0.80  0.40  0.00  98.80  0.00  0.00  0.00
3  1.10  0.20  0.00  98.69  0.00  0.00  0.00
4  0.00  0.00  0.00  100.00  0.00  0.00  0.00
5  2.20  0.00  0.00  97.80  0.00  0.00  0.00
6  0.10  3.20  0.00  96.70  0.00  0.00  0.00
7  0.00  0.00  0.00  100.00  0.00  0.00  0.00

*: interface is up
IHQ: pkts in input hold queue       IQD: pkts dropped from input queue

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
<table>
<thead>
<tr>
<th>Interface</th>
<th>TXBS</th>
<th>TXPS</th>
<th>TRTL</th>
<th>IHQ</th>
<th>IQD</th>
<th>OHQ</th>
<th>OQD</th>
<th>RXBS</th>
<th>RXPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>* GigabitEthernet0/0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/22</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Po1/0/23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>* Po1/0/24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>* Po1/0/25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>* Po1/0/26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Port</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/27</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/28</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/29</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/30</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/31</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fo1/0/32</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/33</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/34</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/35</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/36</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/37</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/38</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/39</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/40</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/41</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/42</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/43</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/44</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/45</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/46</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/47</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HundredGigE1/0/48</td>
<td>0 0 0 0 0 0 0 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASIC 0 Info
-----------

ASIC 0 HSN Table 0 Software info: FSE 255
   TILE 0: (null) srip
   TILE 1: (null) srip

ASIC 0 HSN Table 1 Software info: FSE 255
   TILE 0: (null) srip
   TILE 1: (null) srip

ASIC 0 HSN Table 2 Software info: FSE 0
   TILE 0: Unicast MAC addresses srip 0 1 2 3
   TILE 1: Unicast MAC addresses srip 0 1 2 3

ASIC 0 HSN Table 3 Software info: FSE 0
   TILE 0: Unicast MAC addresses srip 0 1 2 3
   TILE 1: Unicast MAC addresses srip 0 1 2 3

ASIC 0 HSN Table 4 Software info: FSE 255
   TILE 0: (null) srip
   TILE 1: (null) srip

ASIC 0 HSN Table 5 Software info: FSE 255
   TILE 0: (null) srip

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
### OVF Info

---

**Table 0 info:**  
FSE0: 0, FSE1: 255  

#hwmabs: 24, #swmabs: 24

MAB 0: Unicast MAC addresses srip 0 1 2 3  
MAB 1: Unicast MAC addresses srip 0 1 2 3  
MAB 2: Unicast MAC addresses srip 0 1 2 3  
MAB 3: Unicast MAC addresses srip 0 1 2 3  
MAB 4: Unicast MAC addresses srip 0 1 2 3  
MAB 5: Unicast MAC addresses srip 0 1 2 3  
MAB 6: Unicast MAC addresses srip 0 1 2 3  
MAB 7: Unicast MAC addresses srip 0 1 2 3  
MAB 8: Unicast MAC addresses srip 0 1 2 3  
MAB 9: Unicast MAC addresses srip 0 1 2 3
Table 1 info: FSE0: 1, FSE1: 255  #hwmabs: 24, #swmabs: 24

Table 2 info: FSE0: 1, FSE1: 255  #hwmabs: 24, #swmabs: 24
or indirectly connected routes srip 0 1 2 3

Table 3 info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(null)</td>
<td>srip</td>
<td>1</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>2</td>
<td>(null)</td>
<td>srip</td>
<td>3</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>4</td>
<td>(null)</td>
<td>srip</td>
<td>5</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>6</td>
<td>(null)</td>
<td>srip</td>
<td>7</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>8</td>
<td>(null)</td>
<td>srip</td>
<td>9</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>10</td>
<td>(null)</td>
<td>srip</td>
<td>11</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>12</td>
<td>(null)</td>
<td>srip</td>
<td>13</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>14</td>
<td>(null)</td>
<td>srip</td>
<td>15</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>16</td>
<td>(null)</td>
<td>srip</td>
<td>17</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>18</td>
<td>(null)</td>
<td>srip</td>
<td>19</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>20</td>
<td>(null)</td>
<td>srip</td>
<td>21</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>22</td>
<td>(null)</td>
<td>srip</td>
<td>23</td>
<td>(null)</td>
<td>srip</td>
</tr>
</tbody>
</table>

TLQ Info
--------

Table 0 info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(null)</td>
<td>srip</td>
<td>1</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>2</td>
<td>(null)</td>
<td>srip</td>
<td>3</td>
<td>(null)</td>
<td>srip</td>
</tr>
</tbody>
</table>

Table 1 info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
<th>MAB</th>
<th>SGT_DGT</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(null)</td>
<td>srip</td>
<td>1</td>
<td>(null)</td>
<td>srip</td>
</tr>
<tr>
<td>2</td>
<td>(null)</td>
<td>srip</td>
<td>3</td>
<td>(null)</td>
<td>srip</td>
</tr>
</tbody>
</table>

TAQ Info
--------

Table 0 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Input Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 1 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Input Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 2 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 3 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 4 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 5 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Non Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 6 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Non Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Table 7 (TAQ) info:

<table>
<thead>
<tr>
<th>MAB</th>
<th>Output Non Ipv4 Security Access Control Entries</th>
<th>srip</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Table 8 (TAQ) info:

| MAB 0: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 1: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 2: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 3: Output Non Ipv4 Security Access Control Entries srip 1 3 |

Table 9 (TAQ) info:

| MAB 0: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 1: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 2: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 3: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 4: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 5: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 6: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 7: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 8: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 9: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 10: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 11: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 12: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 13: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 14: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 15: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 16: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 17: Input Ipv4 Security Access Control Entries srip 0 2 |
| MAB 18: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 19: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 20: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 21: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 22: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 23: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 24: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 25: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 26: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 27: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 28: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 29: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 30: Input Non Ipv4 Security Access Control Entries srip 0 2 |
| MAB 31: Input Non Ipv4 Security Access Control Entries srip 0 2 |

Table 10 (TAQ) info:

| MAB 0: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 1: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 2: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 3: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 4: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 5: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 6: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 7: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 8: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 9: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 10: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 11: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 12: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 13: Output Ipv4 Security Access Control Entries srip 1 3 |
| MAB 14: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 15: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 16: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 17: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 18: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 19: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 20: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 21: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 22: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 23: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 24: Output Non Ipv4 Security Access Control Entries srip 1 3 |
| MAB 25: Output Non Ipv4 Security Access Control Entries srip 1 3 |
Output Non Ipv4 Security Access Control Entries srip 1 3
MAB 26: Output Non Ipv4 Security Access Control Entries srip 1 3  MAB 27:
Output Non Ipv4 Security Access Control Entries srip 1 3
MAB 28: Output Non Ipv4 Security Access Control Entries srip 1 3  MAB 29:
Output Non Ipv4 Security Access Control Entries srip 1 3
MAB 30: Output Non Ipv4 Security Access Control Entries srip 1 3  MAB 31:

Table 11 (TAQ) info:  ASE: 0  #hwmabs: 4
MAB 0: Input Non Ipv4 Security Access Control Entries srip 0 2  MAB 1: Input Non Ipv4 Security Access Control Entries srip 0 2
MAB 2: Input Non Ipv4 Security Access Control Entries srip 0 2  MAB 3: Input Non Ipv4 Security Access Control Entries srip 0 2

Table 12 (TAQ) info:  ASE: 0  #hwmabs: 4
MAB 0: Input Non Ipv4 Security Access Control Entries srip 0 2  MAB 1: Input Non Ipv4 Security Access Control Entries srip 0 2
MAB 2: Input Non Ipv4 Security Access Control Entries srip 0 2  MAB 3: Input Non Ipv4 Security Access Control Entries srip 0 2

ASIC 1 Info
-------------
ASIC 1 HSN Table 0 Software info:  FSE 255
TILE 0: (null)  srip
TILE 1: (null)  srip
ASIC 1 HSN Table 1 Software info:  FSE 255
TILE 0: (null)  srip
TILE 1: (null)  srip
ASIC 1 HSN Table 2 Software info:  FSE 2
TILE 0: L3 multicast entries srip 0 1 2 3
TILE 1: L3 multicast entries srip 0 1 2 3
ASIC 1 HSN Table 3 Software info:  FSE 2
TILE 0: L3 multicast entries srip 0 1 2 3
TILE 1: L3 multicast entries srip 0 1 2 3
ASIC 1 HSN Table 4 Software info:  FSE 255
TILE 0: (null)  srip
TILE 1: (null)  srip
ASIC 1 HSN Table 5 Software info:  FSE 255
TILE 0: (null)  srip
TILE 1: (null)  srip
ASIC 1 HSN Table 6 Software info:  FSE 1
TILE 0: Directly or indirectly connected routes srip 0 1 2 3
TILE 1: Directly or indirectly connected routes srip 0 1 2 3
ASIC 1 HSN Table 7 Software info:  FSE 1
TILE 0: Directly or indirectly connected routes srip 0 1 2 3
TILE 1: Directly or indirectly connected routes srip 0 1 2 3
ASIC 1 HSF Table 0 Software info:  FSE 1
TILE 0: Directly or indirectly connected routes srip 0 1 2 3
TILE 1: Directly or indirectly connected routes srip 0 1 2 3
TILE 2: Directly or indirectly connected routes srip 0 1 2 3
TILE 3: Directly or indirectly connected routes srip 0 1 2 3
TILE 4: Directly or indirectly connected routes srip 0 1 2 3
TILE 5: Directly or indirectly connected routes srip 0 1 2 3
TILE 6: Directly or indirectly connected routes srip 0 1 2 3
TILE 7: Directly or indirectly connected routes srip 0 1 2 3
ASIC 1 HSF Table 1 Software info:  FSE 1
TILE 0: Directly or indirectly connected routes srip 0 1 2 3
TILE 1: Directly or indirectly connected routes srip 0 1 2 3
TILE 2: Directly or indirectly connected routes srip 0 1 2 3
TILE 3: Directly or indirectly connected routes srip 0 1 2 3
TILE 4: Directly or indirectly connected routes srip 0 1 2 3
TILE 5: Directly or indirectly connected routes srip 0 1 2 3
TILE 6: Directly or indirectly connected routes srip 0 1 2 3
TILE 7: Directly or indirectly connected routes srip 0 1 2 3
ASIC 1 HSF Table 2 Software info:  FSE 1
TILE 0: Directly or indirectly connected routes srip 0 1 2 3
TILE 1: Directly or indirectly connected routes srip 0 1 2 3
TILE 2: Directly or indirectly connected routes srip 0 1 2 3
TILE 3: Directly or indirectly connected routes srip 0 1 2 3
TILE 4: Directly or indirectly connected routes srip 0 1 2 3
TILE 5: Directly or indirectly connected routes srip 0 1 2 3
TILE 6: Directly or indirectly connected routes srip 0 1 2 3
TILE 7: Directly or indirectly connected routes srip 0 1 2 3
### Table 2 info
- FSE0: 1, FSE1: 255
- **#hwmabs**: 24, **#swmabs**: 24
- MAB 0: L2 Multicast entries srip 1 3
- MAB 1: L2 Multicast entries srip 1 3
- MAB 2: L2 Multicast entries srip 1 3
- MAB 3: L2 Multicast entries srip 1 3
- MAB 4: L2 Multicast entries srip 1 3
- MAB 5: L2 Multicast entries srip 1 3
- MAB 6: L2 Multicast entries srip 1 3
- MAB 7: L2 Multicast entries srip 1 3
- MAB 8: L2 Multicast entries srip 1 3
- MAB 9: L2 Multicast entries srip 1 3
- MAB 10: L2 Multicast entries srip 1 3
- MAB 11: L2 Multicast entries srip 1 3
- MAB 12: L2 Multicast entries srip 1 3
- MAB 13: L2 Multicast entries srip 1 3
- MAB 14: L2 Multicast entries srip 1 3
- MAB 15: L2 Multicast entries srip 1 3
- MAB 16: L2 Multicast entries srip 1 3
- MAB 17: L2 Multicast entries srip 1 3
- MAB 18: L2 Multicast entries srip 1 3
- MAB 19: L2 Multicast entries srip 1 3
- MAB 20: L2 Multicast entries srip 1 3
- MAB 21: L2 Multicast entries srip 1 3
- MAB 22: L2 Multicast entries srip 1 3
- MAB 23: L2 Multicast entries srip 1 3

### Table 3 info
- FSE0: 1, FSE1: 255
- **#hwmabs**: 24, **#swmabs**: 24
- MAB 0: L2 Multicast entries srip 1 3
- MAB 1: L2 Multicast entries srip 1 3
- MAB 2: L2 Multicast entries srip 1 3
- MAB 3: L2 Multicast entries srip 1 3
- MAB 4: L2 Multicast entries srip 1 3
- MAB 5: L2 Multicast entries srip 1 3
- MAB 6: L2 Multicast entries srip 1 3
- MAB 7: L2 Multicast entries srip 1 3
- MAB 8: L2 Multicast entries srip 1 3
- MAB 9: L2 Multicast entries srip 1 3
- MAB 10: L2 Multicast entries srip 1 3
- MAB 11: L2 Multicast entries srip 1 3
- MAB 12: L2 Multicast entries srip 1 3
- MAB 13: L2 Multicast entries srip 1 3
- MAB 14: L2 Multicast entries srip 1 3
- MAB 15: L2 Multicast entries srip 1 3
- MAB 16: L2 Multicast entries srip 1 3
- MAB 17: L2 Multicast entries srip 1 3
- MAB 18: L2 Multicast entries srip 1 3
- MAB 19: L2 Multicast entries srip 1 3
- MAB 20: L2 Multicast entries srip 1 3
- MAB 21: L2 Multicast entries srip 1 3
- MAB 22: L2 Multicast entries srip 1 3
- MAB 23: L2 Multicast entries srip 1 3

### TLQ Info

### Table 0 info
- FSE0: 255, FSE1: 255
- **#hwmabs**: 4, **#swmabs**: 4
- MAB 0: (null) srip
- MAB 1: (null) srip
- MAB 2: (null) srip
- MAB 3: (null) srip

### Table 1 info
- FSE0: 255, FSE1: 255
- **#hwmabs**: 4, **#swmabs**: 4
- MAB 0: (null) srip
- MAB 1: (null) srip
- MAB 2: (null) srip
- MAB 3: (null) srip

### TAQ Info

#### Table 0 (TAQ) info
- ASE: 1
- **#hwmabs**: 4
- MAB 0: Ingress Netflow ACEs srip 0 2
- MAB 1: Ingress Netflow ACEs srip 0 2

#### Table 1 (TAQ) info
- ASE: 0
- **#hwmabs**: 4
- MAB 0: Policy Based Routing ACEs srip 0 2
- MAB 1: Policy Based Routing ACEs srip 0 2

#### Table 2 (TAQ) info
- ASE: 0
- **#hwmabs**: 4
- MAB 0: Policy Based Routing ACEs srip 0 2
- MAB 1: Policy Based Routing ACEs srip 0 2

#### Table 3 (TAQ) info
- ASE: 0
- **#hwmabs**: 4
- MAB 0: Policy Based Routing ACEs srip 0 2
- MAB 1: Policy Based Routing ACEs srip 0 2

#### Table 4 (TAQ) info
- ASE: 1
- **#hwmabs**: 4
- MAB 0: Egress Netflow ACEs srip 1 3
- MAB 1: Egress Netflow ACEs srip 1 3

#### Table 5 (TAQ) info
- ASE: 2
- **#hwmabs**: 4
- MAB 0: Flow SPAN ACEs srip 0 2
- MAB 1: Flow SPAN ACEs srip 0 2

#### Table 6 (TAQ) info
- ASE: 7
- **#hwmabs**: 4
- MAB 0: Control Plane Entries srip 1 3
- MAB 1: Control Plane Entries srip 1 3

#### Table 7 (TAQ) info
- ASE: 6
- **#hwmabs**: 4
- MAB 0: Control Plane Entries srip 1 3
- MAB 1: Control Plane Entries srip 1 3
### Table 8 (TAQ) info: ASE: 6 #hwmabs: 4

<table>
<thead>
<tr>
<th>MAB 0: Tunnels srip 0 2</th>
<th>MAB 1: Tunnels srip 0 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAB 2: Tunnels srip 0 2</td>
<td>MAB 3: Tunnels srip 0 2</td>
</tr>
</tbody>
</table>

### Table 9 (TAQ) info: ASE: 3 #hwmabs: 32

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MAB 10: Input Ipv4 QoS Access Control Entries srip 0 2</td>
<td>MAB 11: Input Ipv4 QoS Access Control Entries srip 0 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 10 (TAQ) info: ASE: 3 #hwmabs: 32

<table>
<thead>
<tr>
<th>MAB 0: Output Ipv4 QoS Access Control Entries srip 1 3</th>
<th>MAB 1: Output Ipv4 QoS Access Control Entries srip 1 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAB 2: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 3: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 4: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 5: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 6: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 7: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 8: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 9: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 10: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 11: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 14: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 15: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 16: Output Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 17: Output Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
<tr>
<td>MAB 18: Output Non Ipv4 QoS Access Control Entries srip 1 3</td>
<td>MAB 19: Output Non Ipv4 QoS Access Control Entries srip 1 3</td>
</tr>
</tbody>
</table>

**Note:** The image contains a screenshot of a document page with tables and text, likely related to network configuration or management commands. The tables provide information on various access control entries and their associated capacities. The text also includes references to Cisco IOS XE Gibraltar 16.12.x and Catalyst 9500 switches.
show platform hardware capacity

Table 11 (TAQ) info: ASE: 6 #hwmabs: 4
MAB 0: Tunnels srip 0 2
MAB 1: Tunnels srip 0 2
MAB 2: Tunnels srip 0 2
MAB 3: Macsec SPD srip 1 3

Table 12 (TAQ) info: ASE: 5 #hwmabs: 4
MAB 0: Lisp Instance Mapping Entries srip 0 2
MAB 1: Lisp Instance Mapping Entries srip 0 2
MAB 2: Lisp Instance Mapping Entries srip 0 2
MAB 3: Lisp Instance Mapping Entries srip 0 2
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`

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
</table>
| switch {switch_num | active | standby} | The switch for which you want to display information. You have the following options:
  * switch_num—ID of the switch.
  * active—Displays information relating to the active switch.
  * standby—Displays information relating to the standby switch, if available.

<table>
<thead>
<tr>
<th>forward summary</th>
<th>Displays packet forwarding information.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Support for the keyword <code>summary</code> has been discontinued in the Cisco IOS XE Everest 16.6.1 release and later releases.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (]

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.1 and later releases</td>
<td>Support for the keyword <code>summary</code> was discontinued.</td>
</tr>
</tbody>
</table>

**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
**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
- **hlen** = 6
- **plen** = 4
- **op** = is-at
- **hwsrc** = 00:1d:01:85:ba:22
- **psrc** = 10.10.1.33
- **hwdst** = 00:51:0f:f2:0e:11
- **pdst** = 10.10.1.1

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

Replication Bitmap:
- **Local CPU copy** = 0
- **Local Data copy** = 1
- **Remote CPU copy** = 0
- **Remote Data copy** = 0
Egress:
Switch : 1
Outgoing Port : GigabitEthernet1/0/9
Global Port Number : 9
ASIC Number : 0
Vlan : 1
**show platform hardware fed switch forward interface**

To debug forwarding information and to trace the packet path in the hardware forwarding plane, use the `show platform hardware fed switch switch_number forward interface` command. This command simulates a user-defined packet and retrieves the forwarding information from the hardware forwarding plane. A packet is generated on the ingress port based on the packet parameters that you have specified in this command. You can also provide a complete packet from the captured packets stored in a PCAP file.

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

```
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type interface-number source-mac-address destination-mac-address {protocol-number | arp | cos | ipv4 | ipv6 | mpls}
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type interface-number pcap pcap-file-name number packet-number data
show platform hardware fed switch {switch_num | active | standby} forward interface interface-type interface-number vlan vlan-id source-mac-address destination-mac-address {protocol-number | arp | cos | ipv4 | ipv6 | mpls}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
</table>
| `switch {switch_num | active | standby}` | The switch on which packet tracing has to be scheduled. The input port should be available on this switch. You have the following options:
  - `switch_num`—ID of the switch on which the ingress port is present.
  - `active`—indicates the active switch on which the ingress port is present.
  - `standby`—indicates the standby switch on which the ingress port is present.

  **Note** This keyword is not supported.

| `interface interface-type interface-number` | The input interface on which packet trace is simulated.
| `source-mac-address` | The source MAC address of the packet you want to simulate.
| `destination-mac-address` | The MAC address of the destination interface in hexadecimal format.
| `protocol-number` | The number assigned to any L3 protocol.
| `arp` | The Address Resolution Protocol (ARP) parameters.
| `ipv4` | The IPv4 packet parameters.
| `ipv6` | The IPv6 packet parameters.
| `mpls` | The Multiprotocol Label Switching (MPLS) label parameters. |
The class of service (CoS) number from 0 to 7 to set priority.

**cos**

Name of the pcap file in internal flash (flash:).

**pcap pcap-file-name**

Ensure that the file already exists in flash:.

**number packet-number**

Specifies the packet number in the pcap file.

**number**

VLAN id of the dot1q header in the simulated packet. The range is 1 to 4096.

**vlan vlan-id**

Command Modes

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The command was enhanced to support MPLS/ARP/VxLAN packet parameters and trace packets captured in a PCAP file.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>The command was enhanced to support data capture across a stack.</td>
</tr>
</tbody>
</table>

**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.

This command supports the following packet types:

- Non-IP packets with any L3 protocol
- ARP packets
- IPv4 packets with any L4 protocol
- IPv4 packets with TCP/UDP/IGMP/ICMP/SCTP payload
- VxLAN packets
- MPLS packets with up to 3 Labels and meta data
- MPLS packets with IPv4/IPv6 payload
- IPv6 packets with TCP/UDP/IGMP/ICMP/SCTP payload

In a stack environment, you can trace packets across the stack irrespective of the number of stack members and topology. The `show platform hardware fed switch forward interface switch-number forward interface interface-type interface-number` command consolidates packet-forwarding information of all the stack members on the ingress switch. To achieve this, ensure that the switch number specified in the `switch_num` and `interface-number` arguments are of the input switch and that the number matches.

To trace any particular packet from the captured packets stored in a PCAP file, use the `show platform hardware fed switch forward interface interface-type interface-number pcap pcap-file-name number packet-number data` command.
Example

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

```
Device# show platform hardware fed switch active forward interface gigabitEthernet 1/0/35 0000.0022.0055 0000.0055.0066 ipv4 44.44.0.2 55.55.0.2 udp 1222 3333
```

Show forward is running in the background. After completion, syslog will be generated.

```
*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_DONE: Switch 1 R0/0: fed: Packet Trace Complete: Execute (show platform hardware fed switch <> forward last summary|detail)
*Sep 24 05:57:36.614: %SHFWD-6-PACKET_TRACE_FLOW_ID: Switch 1 R0/0: fed: Packet Trace Flow id is 15032385361
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor capture interface</td>
<td>Configures monitor capture points specifying an attachment point and the packet flow direction.</td>
</tr>
<tr>
<td>monitor capture start</td>
<td>Starts the capture of packet data at a traffic trace point into a buffer.</td>
</tr>
<tr>
<td>monitor capture stop</td>
<td>Stops the capture of packet data at a traffic trace point.</td>
</tr>
<tr>
<td>monitor capture export</td>
<td>Saves the captured packets in the buffer. Use this command to export the monitor capture buffer to a pcap file in flash; that you can use as an input in the <code>show forward</code> with <code>pcap</code>.</td>
</tr>
</tbody>
</table>
**show platform hardware fed switch forward last summary**

To display a summary of packet tracing data from a switch or switches in a stack, use the `show platform hardware fed switch switch_number forward last summary` command.

The output of the `show platform hardware fed switch switch_number forward last summary` command displays all the details about the forwarding decision taken for the packet from the last time the `show forward` command was run.

```
show platform hardware fed switch {switch_number | active | standby} forward last summary
```

**Syntax Description**

| switch  (switch_number | active | standby ) | The switch on which you want to schedule a packet capture for a port. You have the following options:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>switch_num</td>
<td>ID of the switch on which the ingress port is present.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>indicates the active switch on which the ingress port is present.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>standby</td>
<td>indicates the standby switch on which the ingress port is present.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note**

This keyword is not supported.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.1 and later releases</td>
<td>Support for the keyword <code>summary</code> was discontinued.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>Support for keywords <code>last</code> and <code>summary</code> is introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltor 16.10.1</td>
<td>The output of the command was enhanced to display the details about all the copies of the packets and the corresponding outgoing ports.</td>
</tr>
</tbody>
</table>

**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.

With Cisco IOS XE Gibraltor 16.10.1, `show platform hardware fed switch forward last summary` command is enhanced to:

- Inject the debug packets from the CPU to simulate the incoming port and packets
• Use the debug packets to trace the packet in hardware data-path to provide forwarding details such as lookup, adjacency, rewrite information, drop decision, outgoing port and so on
• Drop the original packets at egress so as not to transmit the packet to the outgoing port
• Send a copy of all the packets to the CPU and display the details in the packet tracing output

Example

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

```
Device#show platform hardware fed switch active forward last summary
Ingress Packet Details:
###[ Ethernet ]###
dst = 01:00:5e:01:01:02
src = 00:00:00:03:00:05
type = 0x0
###[ Raw ]###
load = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Ingress:
Port : GigabitEthernet1/0/11
Global Port Number : 11
Local Port Number : 11
Asic Port Number : 10
Asic Instance : 1
Vlan : 20
Mapped Vlan ID : 6
STP Instance : 4
BlockForward : 0
BlockLearn : 0
L3 Interface : 39
IPv4 Routing : enabled
IPv6 Routing : enabled
Vrf Id : 0
Adjacency:
Station Index : 3 [SI_DIET_L2]
Destination Index : 18
Rewrite Index : 2
Replication Bit Map : 0x15 ['localData', 'remoteData', 'coreData']
Decision:
Destination Index : 24 [DI_DIET_L2]
Rewrite Index : 2 [RL_L2]
Dest Mod Index : 9 [DMI_IGMP_CTRL_Q]
CPU Map Index : 0 [CMI_NULL]
Forwarding Mode : 0 [Bridging]
Replication Bit Map : ['localData', 'remoteData', 'coreData']
Winner : L2DESTMACVLAN LOOKUP
Qos Label : 65
SGT : 0
DGTID : 0
Egress:
Possible Replication:
Port : GigabitEthernet1/0/11
Port : GigabitEthernet1/0/22
Port : GigabitEthernet2/0/1
Output Port Data:
Port : GigabitEthernet1/0/22
Global Port Number : 22
```
Local Port Number  : 22
Asic Port Number   : 21
Asic Instance      : 0
Unique RI          : 2
Rewrite Type       : 1 [L2_BRIDGE]
Mapped Rewrite Type: 1 [L2_BRIDGE]
Vlan               : 20
Mapped Vlan ID     : 6
Port               : GigabitEthernet2/0/1
Global Port Number : 97
Local Port Number  : 1
Asic Port Number   : 0
Asic Instance      : 1
Unique RI          : 2
Rewrite Type       : 1 [L2_BRIDGE]
Mapped Rewrite Type: 1 [L2_BRIDGE]
Vlan               : 20
Mapped Vlan ID     : 6

Output Packet Details:
Port               : GigabitEthernet1/0/22
###[ Ethernet ]###
dst                = 01:00:5e:01:01:02
src                = 00:00:00:03:00:05
type               = 0
###[ Raw ]###
load               = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
Port               : GigabitEthernet2/0/1
###[ Ethernet ]###
dst                = 01:00:5e:01:01:02
src                = 00:00:00:03:00:05
type               = 0
###[ Raw ]###
load               = '00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00'
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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

**Example**

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

```
Switch# show platform resources
**State Acronym: H - Healthy, W - Warning, C - Critical

Resource   Usage     Max   Warning   Critical
State
Control Processor  7.20%   100%  90%   95%          H

DRAM         2701MB(69%)  3883MB  90%   95%          H
```

Interface and Hardware Components
show platform software audit

To display the SE Linux Audit logs, use the `show platform software audit` command in privileged EXEC mode.

```
show platform software audit  { all | summary | [ switch {switch-number | active | standby} ] { 0 | F0 | R0 | { FP | RP } ( active ) } }
```

**Syntax Description**

- **all**: Shows the audit log from all the slots.
- **summary**: Shows the audit log summary count from all the slots.
- **switch**: Shows the audit logs for a slot on a specific switch.
- **switch-number**: Selects the switch with the specified switch number.
- **switch active**: Selects the active instance of the switch.
- **standby**: Selects the standby instance of the switch.
- **0**: Shows the audit log for the SPA-Inter-Processor slot 0.
- **F0**: Shows the audit log for the Embedded-Service-Processor slot 0.
- **R0**: Shows the audit log for the Route-Processor slot 0.
- **FP active**: Shows the audit log for the active Embedded-Service-Processor slot.
- **RP active**: Shows the audit log for the active Route-Processor slot.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command was introduced in the Cisco IOS XE Gibraltar 16.10.1 as a part of the SELinux Permissive Mode feature. The `show platform software audit` command displays the system logs containing the access violation events.

In Cisco IOS XE Gibraltar 16.10.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the `show software platform software audit summary` command:
Device# show platform software audit summary

AUDIT LOG ON switch 1

AVC Denial count: 58

The following is a sample output of the `show software platform software audit all` command:

Device# show software platform software audit all

AUDIT LOG ON switch 1

========== START ============
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1

...additional entries...

type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300
comm="sh" name="id" dev="loop0" ino=6982
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1

type=AVC msg=audit(1539438615.535:121): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098
scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1

...additional entries...

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following is a sample output of the `show software platform software audit switch` command:

```
Device# show platform software audit switch active R0

--------- START ---------
```

```
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filter" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0
tclass=lnk_file permissive=1
```

```
type=AVC msg=audit(1539222292.584:101): avc: denied { getattr } for pid=14028
comm="ls" path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0
tclass=dir permissive=1
```

```
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438678.649:124): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438732.973:125): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
type=AVC msg=audit(1539438778.008:126): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0
tclass=file permissive=1
```

```
--------- END ---------
```
show platform software audit

tcontext-system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type-AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext-system_u:system_r:polaris_nginx_t:s0
tcontext-system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
-------------- END --------------

-------------- END --------------
show platform software fed switch punt cpuq rates

To display the rate at which packets are punted, including the drops in the punted path, use the `show platform software fed switch punt cpuq rates` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} punt cpuq rates
```

**Syntax Description**

- `switch{switch-number | active | standby}`
  
  Displays information about the switch. You have the following options:
  
  - `switch-number`.
  - `active`—Displays information relating to the active switch.
  - `standby`—Displays information relating to the standby switch, if available.

  **Note**  This keyword is not supported.

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>punt</code></td>
<td>Specifies the punt information.</td>
</tr>
<tr>
<td><code>cpuq</code></td>
<td>Specifies information about CPU receive queue.</td>
</tr>
<tr>
<td><code>rates</code></td>
<td>Specifies the rate at which the packets are punted.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command displays the rate in packets per second at intervals of 10 seconds, 1 minute and 5 minutes.

**Example**

The following is sample output from the `show platform software fed switch active punt cpuq rates` command.

```
Device#show platform software fed switch active punt cpuq rates

Punt Rate CPU Q Statistics

<table>
<thead>
<tr>
<th>Queue Name</th>
<th>10s</th>
<th>1min</th>
<th>5min</th>
<th>10s</th>
<th>1min</th>
<th>5min</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU_Q_DOT1X_AUTH</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU_Q_L2_CONTROL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CPU_Q_FORUS_TRAFFIC</td>
<td>336</td>
<td>266</td>
<td>320</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The table below describes the significant fields shown in the display.

### Table 9: show platform software fed switch active punt cpuq rates Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Name</td>
<td>Name of the queue.</td>
</tr>
<tr>
<td>Rx</td>
<td>The rate at which the packets are received per second in 10s, 1 minute and 5 minutes.</td>
</tr>
<tr>
<td>Drop</td>
<td>The rate at which the packets are dropped per second in 10s, 1 minute and 5 minutes.</td>
</tr>
</tbody>
</table>
show platform software fed switch punt packet-capture display

To display packet capture information during high CPU utilization, use the `show platform software fed switch active punt packet-capture display` command in privileged EXEC mode.

```
show platform software fed switch active punt packet-capture display { detailed | hexdump }
```

**Syntax Description**

- `switch{switch-number | active | standby}`
  - Displays information about a switch. You have the following options:
    - `active`—Displays information relating to the active switch.
    - `standby`—Displays information relating to the standby switch, if available.
  - **Note** The `standby` keyword is not supported.

- `punt`
  - Specifies punt information.

- `packet-capture display`
  - Specifies information about the captured packet.

- `detailed`
  - Specifies detailed information about the captured packet.

- `hex-dump`
  - Specifies information about the captured packet, in hex format.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command displays the periodic and persistent logs of CPU-bound packets, inband CPU traffic rates, and running CPU processes when the CPU passes a high CPU utilization threshold.

**Examples**

The following is a sample output from the `show platform software fed switch active punt packet-capture display detailed` command:

```
Device# show platform software fed switch active punt packet-capture display detailed
Punt packet capturing: disabled. Buffer wrapping: disabled
Total captured so far: 101 packets. Capture capacity : 4096 packets

interface : GigabitEthernet2/0/2 [if-id: 0x000000032] (physical)
ether hdr : dest mac: 0100.0ccc.cccd, src mac: 2c36.f8fc.4884
ether hdr : ethertype: 0x0032
Doppler Frame Descriptor :
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Packet Data Dump (length: 68 bytes):
01000CCCCCCD2C36 F8FC48840032AAAA 0300000C010B0000 00000080012C36F8
FC48800000000080 012C36F8FC488080 040000140002000F 007100000020001
244E733E

interface: GigabitEthernet2/0/2 [if-id: 0x00000032] (physical)
ether hdr: dest mac: 0180.c200.0000, src mac: 2c36.f8fc.4884
ether hdr: ethertype: 0x0026

show platform software fed switch punt rates interfaces

To display the overall statistics of punt rate for all the interfaces, use the `show platform software fed switch punt rates interfaces` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} punt rates interfaces[interface-id]
```

### Syntax Description

**switch** `{switch-number | active | standby}`

Displays information about the switch. You have the following options:

- `switch-number`
- `active`—Displays information relating to the active switch.
- `standby`—Displays information relating to the standby switch, if available.

**Note**

This keyword is not supported.

**punt**

Specifies the punt information.

**rates**

Specifies the rate at which the packets are punted.

**interfaces[interface-id]**

(Optional) Displays the overall statistics for an interface and also the per-queue configuration for the interface at an interval of 10 seconds.

### Command Modes

Privileged EXEC (#)

### Command History

**Release**

Cisco IOS XE Gibraltar 16.10.1  This command was introduced.

### Usage Guidelines

The output displays the punt rates in packets per second at intervals of 10 seconds, 1 minute and 5 minutes.

### Example

The following is sample output from the `show platform software fed switch active punt rates interfaces` command for all the interfaces.

```
Device#show platform software fed switch active punt rates interfaces

Punt Rate on Interfaces Statistics

Packets per second averaged over 10 seconds, 1 min and 5 mins

<table>
<thead>
<tr>
<th>Interface Name</th>
<th>IF_ID</th>
<th>Rx 10s</th>
<th>Rx 1min</th>
<th>Rx 5min</th>
<th>Drop 10s</th>
<th>Drop 1min</th>
<th>Drop 5min</th>
</tr>
</thead>
</table>
```

---

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**

243
The table below describes the significant fields shown in the display.

Table 10: show platform software fed switch active punt rates interfaces Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Name of the physical interface.</td>
</tr>
<tr>
<td>IF_ID</td>
<td>ID of the physical interface.</td>
</tr>
<tr>
<td>Rx</td>
<td>The per second rate at which the packets are received in 10s, 1 minute and 5 minutes.</td>
</tr>
<tr>
<td>Drop</td>
<td>The per second rate at which the packets are dropped in 10s, 1 minute and 5 minutes.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show platform software fed switch active punt rates interfaces interface-id` command for a specific interface.

```
Device# show platform software fed switch active punt rates interfaces 0x31
Punt Rate on Single Interfaces Statistics
Interface : Port-channel1 [if_id: 0x31]

Received       Dropped
--------------- -------
Total  : 29617 Total : 0
10 sec average : 0 10 sec average : 0
1 min average : 0 1 min average : 0
5 min average : 0 5 min average : 0

Per CPUQ punt stats on the interface (rate averaged over 10s interval)

<table>
<thead>
<tr>
<th>Q</th>
<th>Queue</th>
<th>Recv</th>
<th>Recv</th>
<th>Drop</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
<td>Total</td>
<td>Rate</td>
<td>Total</td>
<td>Rate</td>
</tr>
<tr>
<td>0</td>
<td>CPU_Q_DOT1X_AUTH</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>CPU_Q_L2_CONTROL</td>
<td>29519</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>CPU_Q_FORUS_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>CPU_Q_ICMP_GEN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>CPU_Q_ROUTING_CONTROL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>CPU_Q_FORUS_ADDR_RESOLUTION</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>CPU_Q_ICMP_REDIRECT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>CPU_Q_INTER_FED_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>CPU_Q_L2LXV_CONTROL_PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>CPU_Q_EWLC_CONTROL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>CPU_Q_EWLC_DATA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>CPU_Q_L2LXV_DATA_PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>CPU_Q_BROADCAST</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>CPU_Q_LEARNING_CACHE_OVFL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>CPU_Q_SW_FORWARDING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>CPU_Q_TOPOLOGY_CONTROL</td>
<td>98</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>CPU_Q_PROTO_SNOOPING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>CPU_Q_DHCP_SNOOPING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>CPU_Q_TRANSIT_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>CPU_Q_RPF_FAILED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
The table below describes the significant fields shown in the display.

**Table 11: `show platform software fed switch punt rates interfaces` interface-id Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queue Name</td>
<td>Name of the queue.</td>
</tr>
<tr>
<td>Recv Total</td>
<td>Total number of packets received.</td>
</tr>
<tr>
<td>Recv Rate</td>
<td>Per second rate at which the packets are received.</td>
</tr>
<tr>
<td>Drop Total</td>
<td>Total number of packets dropped.</td>
</tr>
<tr>
<td>Drop Rate</td>
<td>Per second rate at which the packets are dropped.</td>
</tr>
</tbody>
</table>
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.

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

**Syntax Description**
- `details` Displays inline power details for all the interfaces.
- `port` Displays inline power port configuration.
- `GigabitEthernet \interface-number` The GigabitEthernet interface number. Values range from 0 to 9.
- `system slot-number` Displays inline power system configuration.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>

**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
  Signal Pair Power allocation in milli watts: 0
  Spare Pair Power On: 0
  Powered Device power state: 0
  Timer:
```
show platform software ipower

Power Good: Stopped
Power Denied: Stopped
Cisco Powered Device Detect: Stopped
show platform software memory

To display memory information for a specified switch, use the `show platform software memory` command in privileged EXEC mode.

```
show platform software memory [{chunk | database | messaging}] process slot
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chunk</td>
<td>(Optional) Displays chunk memory information for the specified process.</td>
</tr>
<tr>
<td>database</td>
<td>(Optional) Displays database memory information for the specified process.</td>
</tr>
<tr>
<td>messaging</td>
<td>(Optional) Displays messaging memory information for the specified process. The information displayed is for internal debugging purposes only.</td>
</tr>
</tbody>
</table>
show platform software memory

process
Level that is being set. Options include:

- **bt-logger**—The Binary-Tracing Logger process.
- **btrace-manager**—The Btrace Manager process.
- **chassis-manager**—The Chassis Manager process.
- **cli-agent**—The CLI Agent process.
- **cmm**—The CMM process.
- **dbm**—The Database Manager process.
- **dmiauthd**—The DMI Authentication Daemon process.
- **emd**—The Environmental Monitoring process.
- **fed**—The Forwarding Engine Driver process.
- **forwarding-manager**—The Forwarding Manager process.
- **geo**—The Geo Manager process.
- **gnmi**—The GNMI process.
- **host-manager**—The Host Manager process.
- **interface-manager**—The Interface Manager process.
- **iord**—The Input/Output Module daemon (IOMd) process.
- **ios**—The IOS process.
- **iox-manager**—The IOx Manager process.
- **license-manager**—The License Manager process.
- **logger**—The Logging Manager process.
- **mdt-pubd**—The Model Defined Telemetry Publisher process.
- **ndbman**—The Netconf DataBase Manager process.
- **nesd**—The Network Element Synchronizer Daemon process.
- **nginx**—The Nginx Webserver process.
- **nif_mgr**—The NIF 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.
• **syncfd**—The SyncmDaemon process.
• **table-manager**—The Table Manager Server.
• **thread-test**—The Multithread Manager process.
• **virt-manager**—The Virtualization Manager process.

<table>
<thead>
<tr>
<th>slot</th>
<th>Hardware slot where the process for which the level is set, is running. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>* <strong>number</strong>—Number of the SIP slot of the hardware module where the level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.</td>
</tr>
<tr>
<td></td>
<td>* <strong>SIP-slot / SPA-bay</strong>—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.</td>
</tr>
<tr>
<td></td>
<td>* <strong>F0</strong>—The Embedded Service Processor slot 0.</td>
</tr>
<tr>
<td></td>
<td>* <strong>FP active</strong>—The active Embedded Service Processor.</td>
</tr>
<tr>
<td></td>
<td>* <strong>R0</strong>—The route processor in slot 0.</td>
</tr>
<tr>
<td></td>
<td>* <strong>RP active</strong>—The active route processor.</td>
</tr>
<tr>
<td></td>
<td>* <strong>RP standby</strong>—The standby route processor.</td>
</tr>
<tr>
<td></td>
<td>* <strong>switch active</strong>—The active switch.</td>
</tr>
</tbody>
</table>

---

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is a sample output displaying the abbreviated (brief keyword) memory information for the Forwarding Manager process for Cisco Catalyst 9000 Series ESP slot 0:

```
Device# show platform software memory forwarding-manager switch 1 fp active brief

module allocated requested allocs frees
----------------------------------------------
Summary 5702540 5619788 121888 116716
ACM object 1920374 1920310 4 0
ACM links array 880379 880315 4 0
smc_message 819575 819511 4 0
ACM update state 640380 640316 4 0
dpidb-config 208776 203544 351 24
fman-infra-avl 178016 153680 1521 0
ACM batch 152373 152309 4 0
```

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**
The following table describes the significant fields shown in the display.

Table 12: show platform software memory brief Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>module</td>
<td>Name of submodule.</td>
</tr>
<tr>
<td>allocated</td>
<td>Memory, allocated in bytes.</td>
</tr>
<tr>
<td>requested</td>
<td>Number of bytes requested by application.</td>
</tr>
<tr>
<td>allocs</td>
<td>Number of discrete allocation event attempts.</td>
</tr>
<tr>
<td>frees</td>
<td>Number of free events.</td>
</tr>
</tbody>
</table>
To display the list of running processes on a platform, use the show platform software process list command in privileged EXEC mode.

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

**Syntax Description**

- `switch switch-number`: Displays information about the switch. Valid values for `switch-number` argument are from 0 to 9.
- `active`: Displays information about the active instance of the switch.
- `standby`: Displays information about the standby instance of the switch.
- `0`: Displays information about the shared port adapters (SPA) Interface Processor slot 0.
- `F0`: Displays information about the Embedded Service Processor (ESP) slot 0.
- `R0`: Displays information about the Route Processor (RP) slot 0.
- `name process-name`: (Optional) Displays information about the specified process. Enter the process name.
- `process-id process-ID`: (Optional) Displays information about the specified process ID. Enter the 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 EXEC (#)

**Command History**

- **Release**
  - Cisco IOS XE Gibraltar 16.10.1: The Size column in the output was modified to display Resident Set Size (RSS) in KB.
  - Cisco IOS XE Everest 16.5.1a: The command was introduced.

**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
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

The following is sample output from the show platform software process list switch active R0 command:
The table below describes the significant fields shown in the displays.

**Table 13: show platform software process list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the command name associated with the process. Different threads in the same process may have different command values.</td>
</tr>
<tr>
<td>Pid</td>
<td>Displays the process ID that is used by the operating system to identify and keep track of the processes.</td>
</tr>
<tr>
<td>PPid</td>
<td>Displays process ID of the parent process.</td>
</tr>
<tr>
<td>Group Id</td>
<td>Displays the group ID</td>
</tr>
</tbody>
</table>

```plaintext
Device# show platform software process list switch active R0  

<table>
<thead>
<tr>
<th>Name</th>
<th>Pid</th>
<th>PPid</th>
<th>Group Id</th>
<th>Status</th>
<th>Priority</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>systemd</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>S</td>
<td>20</td>
<td>7892</td>
</tr>
<tr>
<td>kthread</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>ksoftirqd/0</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/0:0H</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>rcu_sched</td>
<td>7</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>rcu_bh</td>
<td>8</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>migration/0</td>
<td>9</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>4294967196</td>
<td>0</td>
</tr>
<tr>
<td>migration/1</td>
<td>10</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>4294967196</td>
<td>0</td>
</tr>
<tr>
<td>ksoftirqd/1</td>
<td>11</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/1:0H</td>
<td>13</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>migration/2</td>
<td>14</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>4294967196</td>
<td>0</td>
</tr>
<tr>
<td>ksoftirqd/2</td>
<td>15</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/2:0H</td>
<td>17</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>systemd-journal</td>
<td>221</td>
<td>1</td>
<td>221</td>
<td>S</td>
<td>20</td>
<td>4460</td>
</tr>
<tr>
<td>kworker/1:3</td>
<td>246</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>systemd-udevd</td>
<td>253</td>
<td>1</td>
<td>253</td>
<td>S</td>
<td>20</td>
<td>5648</td>
</tr>
<tr>
<td>kvm-irqfd-clean</td>
<td>617</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>acsi_eh_6</td>
<td>620</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>acsi_tmfs_6</td>
<td>621</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usb-storage</td>
<td>622</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>acsi_eh_7</td>
<td>625</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>acsi_tmfs_7</td>
<td>626</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>usb-storage</td>
<td>627</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/7:1</td>
<td>630</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>bioset</td>
<td>631</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/3:1H</td>
<td>648</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/0:1H</td>
<td>667</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/1:1H</td>
<td>668</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>bioset</td>
<td>669</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/6:2</td>
<td>698</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/2:2</td>
<td>699</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>kworker/2:1H</td>
<td>703</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/7:1H</td>
<td>748</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/5:1H</td>
<td>749</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/6:1H</td>
<td>754</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>kworker/7:2</td>
<td>779</td>
<td>2</td>
<td>0</td>
<td>S</td>
<td>20</td>
<td>0</td>
</tr>
<tr>
<td>auditd</td>
<td>838</td>
<td>1</td>
<td>838</td>
<td>S</td>
<td>16</td>
<td>2564</td>
</tr>
</tbody>
</table>
```
### show platform software process list

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Displays the process status in human readable form.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the negated scheduling priority.</td>
</tr>
<tr>
<td>Size</td>
<td>Prior to Cisco IOS XE Gibraltar 16.10.1: Displays Virtual Memory size.</td>
</tr>
<tr>
<td></td>
<td>From Cisco IOS XE Gibraltar 16.10.1 onwards: Displays the Resident Set Size (RSS) that shows how much memory is allocated to that process in the RAM.</td>
</tr>
</tbody>
</table>
show platform software process memory

To display the amount of memory used by each system process, use the `show platform software process memory` command in privileged EXEC mode.

```plaintext
show platform software process memory
switch {switch-number | active | standby} {0 | F0 | FP | R0} {all | sorted | virtual [sorted]} | name process-name {maps | smaps [summary]} | process-id process-id {maps | smaps [summary]} }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch switch-number</code></td>
<td>Displays information about the switch. Enter the switch number.</td>
</tr>
<tr>
<td><code>active</code></td>
<td>Specifies the active instance of the device.</td>
</tr>
<tr>
<td><code>standby</code></td>
<td>Specifies the standby instance of the device.</td>
</tr>
<tr>
<td><code>0</code></td>
<td>Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.</td>
</tr>
<tr>
<td><code>F0</code></td>
<td>Specifies the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td><code>FP</code></td>
<td>Specifies the Embedded Service Processor (ESP).</td>
</tr>
<tr>
<td><code>R0</code></td>
<td>Specifies the Route Processor (RP) slot 0.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Lists all processes.</td>
</tr>
<tr>
<td><code>sorted</code></td>
<td>(Optional) Sorts the output based on Resident Set Size (RSS).</td>
</tr>
<tr>
<td><code>virtual</code></td>
<td>(Optional) Specifies virtual memory.</td>
</tr>
<tr>
<td><code>name process-name</code></td>
<td>Specifies a process name.</td>
</tr>
<tr>
<td><code>maps</code></td>
<td>Specifies the memory maps of a process.</td>
</tr>
<tr>
<td><code>smaps summary</code></td>
<td>Specifies the smaps summary of a process.</td>
</tr>
<tr>
<td><code>process-id process-id</code></td>
<td>Specifies a process identifier.</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC(#) | 

### Examples:

The following is a sample output from the `show platform software process memory active R0 all` command:
Device# show platform software process memory switch active R0 all

<table>
<thead>
<tr>
<th>Pid</th>
<th>RSS</th>
<th>PSS</th>
<th>Heap</th>
<th>Shared</th>
<th>Private</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4876</td>
<td>3229</td>
<td>1064</td>
<td>1808</td>
<td>3068</td>
<td>systemd</td>
</tr>
<tr>
<td>118</td>
<td>3184</td>
<td>1327</td>
<td>132</td>
<td>2352</td>
<td>832</td>
<td>systemd-journal</td>
</tr>
<tr>
<td>159</td>
<td>3008</td>
<td>1191</td>
<td>396</td>
<td>1996</td>
<td>1012</td>
<td>systemd-udevd</td>
</tr>
<tr>
<td>407</td>
<td>3192</td>
<td>1262</td>
<td>132</td>
<td>2196</td>
<td>996</td>
<td>dbus-daemon</td>
</tr>
<tr>
<td>3406</td>
<td>4772</td>
<td>3064</td>
<td>264</td>
<td>1940</td>
<td>2832</td>
<td>virtlogd</td>
</tr>
<tr>
<td>3411</td>
<td>5712</td>
<td>3474</td>
<td>2964</td>
<td>2344</td>
<td>3368</td>
<td>systemd-udevd</td>
</tr>
<tr>
<td>3416</td>
<td>2588</td>
<td>358</td>
<td>132</td>
<td>2336</td>
<td>252</td>
<td>libvirtd</td>
</tr>
<tr>
<td>3420</td>
<td>5708</td>
<td>3484</td>
<td>2976</td>
<td>2308</td>
<td>3400</td>
<td>reflector.sh</td>
</tr>
<tr>
<td>3424</td>
<td>1804</td>
<td>263</td>
<td>132</td>
<td>1632</td>
<td>172</td>
<td>xinetd</td>
</tr>
<tr>
<td>3425</td>
<td>964</td>
<td>118</td>
<td>132</td>
<td>872</td>
<td>92</td>
<td>sleep</td>
</tr>
<tr>
<td>3434</td>
<td>3060</td>
<td>844</td>
<td>528</td>
<td>2304</td>
<td>756</td>
<td>oom.sh</td>
</tr>
<tr>
<td>3442</td>
<td>2068</td>
<td>606</td>
<td>132</td>
<td>1604</td>
<td>464</td>
<td>rpcbind</td>
</tr>
<tr>
<td>3485</td>
<td>2380</td>
<td>845</td>
<td>132</td>
<td>1636</td>
<td>744</td>
<td>rpc.statd</td>
</tr>
<tr>
<td>3486</td>
<td>1632</td>
<td>338</td>
<td>132</td>
<td>1348</td>
<td>284</td>
<td>boothelper_evt.</td>
</tr>
<tr>
<td>3493</td>
<td>1136</td>
<td>156</td>
<td>132</td>
<td>1004</td>
<td>132</td>
<td>inotifywait</td>
</tr>
<tr>
<td>3504</td>
<td>2048</td>
<td>753</td>
<td>132</td>
<td>1372</td>
<td>676</td>
<td>rpc.mountd</td>
</tr>
<tr>
<td>3584</td>
<td>2868</td>
<td>620</td>
<td>36</td>
<td>2384</td>
<td>484</td>
<td>rotee</td>
</tr>
<tr>
<td>3649</td>
<td>1032</td>
<td>116</td>
<td>132</td>
<td>944</td>
<td>88</td>
<td>sleep</td>
</tr>
<tr>
<td>3705</td>
<td>2784</td>
<td>613</td>
<td>36</td>
<td>2296</td>
<td>488</td>
<td>rotee</td>
</tr>
<tr>
<td>3718</td>
<td>2856</td>
<td>610</td>
<td>36</td>
<td>2376</td>
<td>480</td>
<td>rotee</td>
</tr>
<tr>
<td>3759</td>
<td>1292</td>
<td>184</td>
<td>132</td>
<td>1136</td>
<td>156</td>
<td>inotifywait</td>
</tr>
<tr>
<td>3787</td>
<td>4256</td>
<td>2040</td>
<td>1640</td>
<td>2300</td>
<td>1956</td>
<td>iptbl.sh</td>
</tr>
<tr>
<td>3894</td>
<td>2948</td>
<td>637</td>
<td>36</td>
<td>2460</td>
<td>488</td>
<td>rotee</td>
</tr>
<tr>
<td>4017</td>
<td>1380</td>
<td>175</td>
<td>132</td>
<td>1236</td>
<td>144</td>
<td>inotifywait</td>
</tr>
<tr>
<td>4866</td>
<td>1820</td>
<td>287</td>
<td>132</td>
<td>1624</td>
<td>196</td>
<td>xinetd</td>
</tr>
<tr>
<td>5887</td>
<td>1692</td>
<td>257</td>
<td>132</td>
<td>1508</td>
<td>184</td>
<td>xinetd</td>
</tr>
<tr>
<td>5891</td>
<td>7248</td>
<td>4984</td>
<td>4584</td>
<td>2348</td>
<td>4900</td>
<td>rollback_timer.</td>
</tr>
<tr>
<td>5893</td>
<td>1764</td>
<td>257</td>
<td>132</td>
<td>1588</td>
<td>176</td>
<td>xinetd</td>
</tr>
<tr>
<td>6031</td>
<td>2804</td>
<td>601</td>
<td>36</td>
<td>2332</td>
<td>472</td>
<td>rotee</td>
</tr>
<tr>
<td>6037</td>
<td>1228</td>
<td>163</td>
<td>132</td>
<td>1092</td>
<td>136</td>
<td>inotifywait</td>
</tr>
<tr>
<td>6077</td>
<td>4736</td>
<td>3389</td>
<td>2992</td>
<td>1368</td>
<td>3368</td>
<td>pysp.sh</td>
</tr>
<tr>
<td>6115</td>
<td>1620</td>
<td>476</td>
<td>36</td>
<td>1152</td>
<td>468</td>
<td>rotee</td>
</tr>
<tr>
<td>6122</td>
<td>624</td>
<td>149</td>
<td>132</td>
<td>480</td>
<td>144</td>
<td>inotifywait</td>
</tr>
<tr>
<td>6127</td>
<td>5440</td>
<td>4077</td>
<td>3680</td>
<td>1384</td>
<td>4056</td>
<td>pysp.sh</td>
</tr>
<tr>
<td>6165</td>
<td>1736</td>
<td>592</td>
<td>36</td>
<td>1152</td>
<td>584</td>
<td>rotee</td>
</tr>
<tr>
<td>6245</td>
<td>624</td>
<td>149</td>
<td>132</td>
<td>480</td>
<td>144</td>
<td>inotifywait</td>
</tr>
<tr>
<td>6353</td>
<td>2592</td>
<td>1260</td>
<td>924</td>
<td>1352</td>
<td>1240</td>
<td>pman.sh</td>
</tr>
<tr>
<td>6470</td>
<td>1632</td>
<td>488</td>
<td>36</td>
<td>1152</td>
<td>480</td>
<td>rotee</td>
</tr>
<tr>
<td>6499</td>
<td>2588</td>
<td>1262</td>
<td>924</td>
<td>1348</td>
<td>1240</td>
<td>pman.sh</td>
</tr>
<tr>
<td>6666</td>
<td>1640</td>
<td>496</td>
<td>36</td>
<td>1152</td>
<td>488</td>
<td>rotee</td>
</tr>
<tr>
<td>6718</td>
<td>2584</td>
<td>1258</td>
<td>800</td>
<td>1348</td>
<td>1236</td>
<td>pman.sh</td>
</tr>
<tr>
<td>6736</td>
<td>8360</td>
<td>7020</td>
<td>6640</td>
<td>1360</td>
<td>7000</td>
<td>auto_upgrade_cl</td>
</tr>
<tr>
<td>6909</td>
<td>1636</td>
<td>492</td>
<td>36</td>
<td>1152</td>
<td>484</td>
<td>rotee</td>
</tr>
<tr>
<td>6955</td>
<td>2588</td>
<td>1262</td>
<td>928</td>
<td>1348</td>
<td>1240</td>
<td>pman.sh</td>
</tr>
<tr>
<td>7029</td>
<td>2196</td>
<td>679</td>
<td>40</td>
<td>1552</td>
<td>644</td>
<td>auto_upgrade_se</td>
</tr>
<tr>
<td>7149</td>
<td>1636</td>
<td>492</td>
<td>36</td>
<td>1152</td>
<td>484</td>
<td>rotee</td>
</tr>
<tr>
<td>7224</td>
<td>13200</td>
<td>4595</td>
<td>48</td>
<td>9368</td>
<td>3832</td>
<td>bt_logger</td>
</tr>
<tr>
<td>7295</td>
<td>2588</td>
<td>1262</td>
<td>800</td>
<td>1348</td>
<td>1240</td>
<td>pman.sh</td>
</tr>
</tbody>
</table>

The table below describes the significant fields shown in the displays.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PID</td>
<td>Displays the process ID that is used by the operating system to identify and keep track of the processes.</td>
</tr>
<tr>
<td>RSS</td>
<td>Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.</td>
</tr>
<tr>
<td>PSS</td>
<td>Displays the Proportional Set Size of a process. This is the count of pages it has in memory, where each page is divided by the number of processes sharing it.</td>
</tr>
<tr>
<td>Heap</td>
<td>Displays where all user-allocated memory is located.</td>
</tr>
<tr>
<td>Shared</td>
<td>Shared clean + Shared dirty</td>
</tr>
<tr>
<td>Private</td>
<td>Private clean + Private dirty</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the command name associated with the process. Different threads in the same process may have different command values.</td>
</tr>
</tbody>
</table>
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

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

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```
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

<table>
<thead>
<tr>
<th>PID</th>
<th>USER</th>
<th>PR</th>
<th>NI</th>
<th>VIRT</th>
<th>RES</th>
<th>SHR</th>
<th>S</th>
<th>%CPU</th>
<th>%MEM</th>
<th>TIME+</th>
<th>COMMAND</th>
</tr>
</thead>
<tbody>
<tr>
<td>5693</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>3448</td>
<td>1368</td>
<td>912</td>
<td>R</td>
<td>7</td>
<td>0.0</td>
<td>0:00.07</td>
<td>top</td>
</tr>
<tr>
<td>17546</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>2044m</td>
<td>244m</td>
<td>79m</td>
<td>S</td>
<td>7</td>
<td>6.3</td>
<td>186:49:08</td>
<td>fed main event</td>
</tr>
<tr>
<td>18662</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>1806m</td>
<td>678m</td>
<td>263m</td>
<td>S</td>
<td>5</td>
<td>17.5</td>
<td>215:32:38</td>
<td>linux_iosd-imag</td>
</tr>
<tr>
<td>30276</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>171m</td>
<td>42m</td>
<td>33m</td>
<td>S</td>
<td>5</td>
<td>1.1</td>
<td>125:06:77</td>
<td>repm</td>
</tr>
<tr>
<td>17835</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>935m</td>
<td>74m</td>
<td>63m</td>
<td>S</td>
<td>4</td>
<td>1.9</td>
<td>82:28:31</td>
<td>sif_mgr</td>
</tr>
<tr>
<td>18534</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>182m</td>
<td>150m</td>
<td>10m</td>
<td>S</td>
<td>2</td>
<td>3.9</td>
<td>8:12:08</td>
<td>smand</td>
</tr>
<tr>
<td>1</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>4740</td>
<td>2184</td>
<td>S</td>
<td>0</td>
<td>0.1</td>
<td>0:09:52</td>
<td>systemd</td>
</tr>
<tr>
<td>2</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kthread</td>
</tr>
<tr>
<td>3</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:02.86</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>5</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>kworker/0:0H</td>
</tr>
<tr>
<td>7</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:01.44</td>
<td>migration/0</td>
</tr>
<tr>
<td>8</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:00.00</td>
<td>rcu_bh</td>
</tr>
<tr>
<td>9</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:23.08</td>
<td>rcu_sched</td>
</tr>
<tr>
<td>10</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:58:04</td>
<td>rcuc/0</td>
</tr>
<tr>
<td>11</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>21:35:60</td>
<td>rcuc/1</td>
</tr>
<tr>
<td>12</td>
<td>root</td>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>0.0</td>
<td>0:01:33</td>
<td>migration/1</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show processes cpu platform monitor location</code></td>
<td>Displays information about the CPU utilization of the IOS-XE processes.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
   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)
```
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
<table>
<thead>
<tr>
<th>Slot</th>
<th>Status</th>
<th>1-Min</th>
<th>5-Min</th>
<th>15-Min</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-RP0</td>
<td>Healthy</td>
<td>1.10</td>
<td>1.21</td>
<td>0.91</td>
</tr>
<tr>
<td>3-RP0</td>
<td>Healthy</td>
<td>0.23</td>
<td>0.27</td>
<td>0.31</td>
</tr>
<tr>
<td>4-RP0</td>
<td>Healthy</td>
<td>0.11</td>
<td>0.21</td>
<td>0.22</td>
</tr>
<tr>
<td>9-RP0</td>
<td>Healthy</td>
<td>0.10</td>
<td>0.30</td>
<td>0.34</td>
</tr>
</tbody>
</table>

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

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

To display the list of threads on a platform, use the `show platform software thread list` command in privileged EXEC mode.

```
show platform software thread list switch { switch-number | active | standby } { 0 | F0 | FP active | R0 } pname { cdman | vidman | all } tname { main | pktio | rt | all }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch switch-number</td>
<td>Displays information about the switch. Enter the switch number.</td>
</tr>
<tr>
<td>active</td>
<td>Specifies the active instance of the device.</td>
</tr>
<tr>
<td>standby</td>
<td>Specifies standby instance of the device.</td>
</tr>
<tr>
<td>0</td>
<td>Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.</td>
</tr>
<tr>
<td>F0</td>
<td>Specifies the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td>FP active</td>
<td>Specifies the active instance of Embedded Service Processor (ESP).</td>
</tr>
<tr>
<td>R0</td>
<td>Specifies the Route Processor (RP) slot 0.</td>
</tr>
<tr>
<td>pname</td>
<td>Specifies a process name. The possible values are cdman, vidman, and all.</td>
</tr>
<tr>
<td>tname</td>
<td>Specifies a thread name. The possible values are main, pktio, rt, and all.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC(##)

**Examples:**

The following is sample output from the `show platform software thread list switch active R0 pname cdman tname all` command:

```
Device# show platform software thread list switch active R0 pname cdman tname all

Name   Tid   PPid  Group Id  Core  Vcawch  Nvcawch  Status  Priority
------  -----  -----  ---------  -----  --------  --------  -------  ---------
  cdman   8407    7295    8407   1     0        0       S        20

12309   36976
```

The table below describes the significant fields shown in the displays.
### Table 15: show platform software thread list Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the command name associated with the process. Different threads in the same process may have different command values.</td>
</tr>
<tr>
<td>Tid</td>
<td>Displays the process ID.</td>
</tr>
<tr>
<td>PPid</td>
<td>Displays the process ID of the parent process.</td>
</tr>
<tr>
<td>Group Id</td>
<td>Displays the group ID.</td>
</tr>
<tr>
<td>Core</td>
<td>Displays processor information.</td>
</tr>
<tr>
<td>Vcswch</td>
<td>Displays the number of voluntary context switches.</td>
</tr>
<tr>
<td>Nvcswch</td>
<td>Displays the number of non-voluntary context switches.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the process status in human readable form.</td>
</tr>
<tr>
<td>Priority</td>
<td>Displays the negated scheduling priority.</td>
</tr>
<tr>
<td>TIME+</td>
<td>Displays the time since the start of the process.</td>
</tr>
<tr>
<td>Size</td>
<td>Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.</td>
</tr>
</tbody>
</table>
show processes cpu platform

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

```
show processes cpu platform  [[ sorted [1min | 5min | 5sec] ] location
switch {switch-number | active | standby} {F0 | FP active | R0 | RP active}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sorted</td>
<td>(Optional) Displays output sorted based on percentage of CPU usage on a platform.</td>
</tr>
<tr>
<td>1min</td>
<td>(Optional) Sorts based on 1 minute intervals.</td>
</tr>
<tr>
<td>5min</td>
<td>(Optional) Sorts based on 5 minute intervals.</td>
</tr>
<tr>
<td>5sec</td>
<td>(Optional) Sorts based on 5 second intervals.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the Field Replaceable Unit (FRU) location.</td>
</tr>
<tr>
<td>switch</td>
<td>Displays information about the switch. Enter the switch number.</td>
</tr>
<tr>
<td>switch-number</td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>Specifies the active instance of the device.</td>
</tr>
<tr>
<td>standby</td>
<td>Specifies the standby instance of the device.</td>
</tr>
<tr>
<td>F0</td>
<td>Specifies the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td>FP active</td>
<td>Specifies active instances on the Embedded Service Processor (ESP).</td>
</tr>
<tr>
<td>R0</td>
<td>Specifies the Route Processor (RP) slot 0.</td>
</tr>
<tr>
<td>RP active</td>
<td>Specifies active instances on the Route Processor (RP).</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Examples:

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

```
Device# show processes cpu platform

CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 2%
Core 0: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 3%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 2%, one minute: 5%, five minutes: 2%
  Pid  PPid  5Sec  1Min  5Min Status  Size  Name
  -----------------------------------------------
    1  0  0%  0%  0%  S  4876  systemd
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 0: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 1: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 1%
Core 4: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 5: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 6: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 7: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%

<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Status</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>16358</td>
<td>15516</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
<td>S</td>
<td>221376</td>
<td>fed main event</td>
</tr>
<tr>
<td>14062</td>
<td>12756</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>S</td>
<td>52140</td>
<td>sif_mgr</td>
</tr>
<tr>
<td>32105</td>
<td>8618</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>260</td>
<td>inotifywait</td>
</tr>
<tr>
<td>31396</td>
<td>31393</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>36516</td>
<td>python2.7</td>
</tr>
<tr>
<td>31393</td>
<td>31271</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2744</td>
<td>rdope.sh</td>
</tr>
<tr>
<td>31319</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2648</td>
<td>rotee</td>
</tr>
<tr>
<td>31271</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3852</td>
<td>pman.sh</td>
</tr>
<tr>
<td>29671</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2788</td>
<td>stack_sntp.sh</td>
</tr>
<tr>
<td>29341</td>
<td>29329</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>1780</td>
<td>stack_sntp.sh</td>
</tr>
<tr>
<td>29329</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2788</td>
<td>stack_sntp.sh</td>
</tr>
</tbody>
</table>

The following is sample output from the `show processes cpu platform sorted 5min location switch 5 R0` command.
The following is sample output from the `show processes cpu platform location switch 7 R0` command:

```
Device# show processes cpu platform location switch 7 R0

CPU utilization for five seconds: 3%, one minute: 3%, five minutes: 3%
Core 0: CPU utilization for five seconds: 1%, one minute: 5%, five minutes: 5%
Core 1: CPU utilization for five seconds: 1%, one minute: 11%, five minutes: 5%
Core 2: CPU utilization for five seconds: 22%, one minute: 7%, five minutes: 6%
Core 3: CPU utilization for five seconds: 5%, one minute: 6%, five minutes: 6%
Core 4: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 5: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 6: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 0%
Core 7: CPU utilization for five seconds: 0%, one minute: 0%, five minutes: 6%
```

```
<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Status</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>8044 systemd</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0 kthreadd</td>
</tr>
</tbody>
</table>
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show processes cpu platform history

To display information about the CPU usage history of a system, use the `show processes cpu platform history` command.

```
show processes cpu platform history [1min | 5min | 5sec | 60min] location
switch [switch-number | active | standby | 0 | F0 | FP active | R0]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1min</td>
<td>(Optional) Displays CPU utilization history with 1 minute intervals.</td>
</tr>
<tr>
<td>5min</td>
<td>(Optional) Displays CPU utilization history with 5 minute intervals.</td>
</tr>
<tr>
<td>5sec</td>
<td>(Optional) Displays CPU utilization history with 5 second intervals.</td>
</tr>
<tr>
<td>60min</td>
<td>(Optional) Displays CPU utilization history with 60 minute intervals.</td>
</tr>
<tr>
<td>location</td>
<td>Specifies the Field Replaceable Unit (FRU) location.</td>
</tr>
<tr>
<td>switch</td>
<td>Displays information about the switch. Enter the switch number.</td>
</tr>
<tr>
<td>switch-number</td>
<td></td>
</tr>
<tr>
<td>active</td>
<td>Specifies the active instance of the device.</td>
</tr>
<tr>
<td>standby</td>
<td>Specifies the standby instance of the device.</td>
</tr>
<tr>
<td>0</td>
<td>Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.</td>
</tr>
<tr>
<td>F0</td>
<td>Specifies the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td>FP active</td>
<td>Specifies active instances on the Embedded Service Processor (ESP).</td>
</tr>
<tr>
<td>R0</td>
<td>Specifies the Route Processor (RP) slot 0.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Examples:**

The following is sample output from the `show processes cpu platform` command:

```
Device# show processes cpu platform
```
CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 2%
Core 0: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 2: CPU utilization for five seconds: 3%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 2%, one minute: 5%, five minutes: 2%

```
<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Status</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>4876</td>
<td>systemd</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kthreadd</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>rcu_sched</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>rcu_bh</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>migration/0</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>watchdog/0</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>watchdog/1</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>migration/1</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/1</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/1:0H</td>
</tr>
<tr>
<td>16</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>watchdog/2</td>
</tr>
<tr>
<td>17</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>migration/2</td>
</tr>
<tr>
<td>18</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/2</td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/2:0H</td>
</tr>
<tr>
<td>22</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>watchd/bg/3</td>
</tr>
<tr>
<td>23</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/3</td>
</tr>
<tr>
<td>24</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/3:0</td>
</tr>
<tr>
<td>25</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/3:0H</td>
</tr>
<tr>
<td>26</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kdevtmpfs</td>
</tr>
<tr>
<td>27</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>netns</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>perf</td>
</tr>
<tr>
<td>29</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>khungtaskd</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>writeback</td>
</tr>
<tr>
<td>31</td>
<td>2</td>
<td>7%</td>
<td>8%</td>
<td>8%</td>
<td>S</td>
<td>0</td>
<td>kadm</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>khugepaged</td>
</tr>
<tr>
<td>33</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>crypto</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>bioet</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kblockd</td>
</tr>
<tr>
<td>36</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>ata_sff</td>
</tr>
<tr>
<td>37</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>rpciod</td>
</tr>
<tr>
<td>63</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kswapd0</td>
</tr>
<tr>
<td>64</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>vmmstat</td>
</tr>
<tr>
<td>65</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>fsnotify_mark</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show processes cpu platform history 5sec` command:

```
Device# show processes cpu platform history 5sec

5 seconds ago, CPU utilization: 0%
10 seconds ago, CPU utilization: 0%
15 seconds ago, CPU utilization: 0%
20 seconds ago, CPU utilization: 0%
25 seconds ago, CPU utilization: 0%
30 seconds ago, CPU utilization: 0%
35 seconds ago, CPU utilization: 0%
40 seconds ago, CPU utilization: 0%
45 seconds ago, CPU utilization: 0%
50 seconds ago, CPU utilization: 0%
55 seconds ago, CPU utilization: 0%
60 seconds ago, CPU utilization: 0%
65 seconds ago, CPU utilization: 0%
70 seconds ago, CPU utilization: 0%
```
75 seconds ago, CPU utilization: 0%
80 seconds ago, CPU utilization: 0%
85 seconds ago, CPU utilization: 0%
90 seconds ago, CPU utilization: 0%
95 seconds ago, CPU utilization: 0%
100 seconds ago, CPU utilization: 0%
105 seconds ago, CPU utilization: 0%
110 seconds ago, CPU utilization: 0%
115 seconds ago, CPU utilization: 0%
120 seconds ago, CPU utilization: 0%
125 seconds ago, CPU utilization: 0%
130 seconds ago, CPU utilization: 0%
135 seconds ago, CPU utilization: 0%
140 seconds ago, CPU utilization: 0%
145 seconds ago, CPU utilization: 0%
150 seconds ago, CPU utilization: 0%
155 seconds ago, CPU utilization: 0%
160 seconds ago, CPU utilization: 0%
165 seconds ago, CPU utilization: 0%
170 seconds ago, CPU utilization: 0%
175 seconds ago, CPU utilization: 0%
180 seconds ago, CPU utilization: 0%
185 seconds ago, CPU utilization: 0%
190 seconds ago, CPU utilization: 0%
195 seconds ago, CPU utilization: 0%
200 seconds ago, CPU utilization: 0%
205 seconds ago, CPU utilization: 0%
210 seconds ago, CPU utilization: 0%
215 seconds ago, CPU utilization: 0%
220 seconds ago, CPU utilization: 0%
225 seconds ago, CPU utilization: 0%
230 seconds ago, CPU utilization: 0%
235 seconds ago, CPU utilization: 0%
240 seconds ago, CPU utilization: 0%
245 seconds ago, CPU utilization: 0%
250 seconds ago, CPU utilization: 0%
.
show processes cpu platform monitor

To display 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**

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

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 0:00.07 top
17546 root 20 0 2044m 244m 79m S 7 6.3 187:02.07 fed main event
30276 root 20 0 171m 42m 33m S 7 1.1 125:15.54 repm
16 root 20 0 0 0 0 S 5 0.0 22:07.92 rcuc/2
21 root 20 0 0 0 0 R 5 0.0 22:13.24 rcuc/3
```
show processes cpu platform monitor

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform software process slot switch</td>
<td>Displays platform software process switch information.</td>
</tr>
</tbody>
</table>
To display memory usage for each Cisco IOS XE process, use the `show processes memory platform` command in privileged EXEC mode.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>(Optional) Displays the top memory allocators for each Cisco IOS XE process.</td>
</tr>
<tr>
<td>detailed</td>
<td>(Optional) Displays detailed memory information for a specified Cisco IOS XE process.</td>
</tr>
<tr>
<td>name process-name</td>
<td>(Optional) Displays the Cisco IOS XE process name. Enter the process name.</td>
</tr>
<tr>
<td>process-id process-ID</td>
<td>(Optional) Displays the Cisco IOS XE process ID. Enter the process ID.</td>
</tr>
<tr>
<td>location</td>
<td>(Optional) Displays information about the Field Replaceable Unit (FRU) location.</td>
</tr>
<tr>
<td>maps</td>
<td>(Optional) Displays memory maps of a process.</td>
</tr>
<tr>
<td>smaps</td>
<td>(Optional) Displays static memory maps of a process.</td>
</tr>
<tr>
<td>sorted</td>
<td>(Optional) Displays the sorted output based on the Resident Set Size (RSS) memory used by Cisco IOS XE process.</td>
</tr>
<tr>
<td>switch switch-number</td>
<td>Displays information about the device.</td>
</tr>
<tr>
<td>active</td>
<td>Displays information about the active instance of the device.</td>
</tr>
<tr>
<td>standby</td>
<td>Displays information about the standby instance of the device.</td>
</tr>
<tr>
<td>0</td>
<td>Displays information about Shared Port Adapter (SPA)-Inter-Processor slot 0.</td>
</tr>
<tr>
<td>F0</td>
<td>Displays information about Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td>R0</td>
<td>Displays information about Route Processor (RP) slot 0.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
### Modification

**Release**
Cisco IOS XE Gibraltar 16.10.1

**Modification**
This command was modified. The keyword `accounting` was added. The `Total` column was deleted from the output.

### Examples

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

```
device# show processes memory platform

System memory: 3976852K total, 2761580K used, 1215272K free,
Lowest: 1215272K

<table>
<thead>
<tr>
<th>Pid</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1246</td>
<td>4400</td>
<td>132</td>
<td>1308</td>
<td>4400</td>
<td>systemd</td>
</tr>
<tr>
<td>96</td>
<td>233</td>
<td>2796</td>
<td>132</td>
<td>132</td>
<td>2796</td>
<td>systemd-udevd</td>
</tr>
<tr>
<td>105</td>
<td>284</td>
<td>1796</td>
<td>132</td>
<td>176</td>
<td>1796</td>
<td>in.telnetd</td>
</tr>
<tr>
<td>707</td>
<td>52</td>
<td>2660</td>
<td>132</td>
<td>172</td>
<td>2660</td>
<td>brelay.sh</td>
</tr>
<tr>
<td>744</td>
<td>968</td>
<td>3264</td>
<td>132</td>
<td>1700</td>
<td>3264</td>
<td>in.telnetd</td>
</tr>
<tr>
<td>835</td>
<td>52</td>
<td>2660</td>
<td>132</td>
<td>172</td>
<td>2660</td>
<td>brelay.sh</td>
</tr>
<tr>
<td>863</td>
<td>968</td>
<td>3264</td>
<td>132</td>
<td>1700</td>
<td>3264</td>
<td>reflector.sh</td>
</tr>
<tr>
<td>928</td>
<td>968</td>
<td>3996</td>
<td>132</td>
<td>2312</td>
<td>3996</td>
<td>droputil.sh</td>
</tr>
<tr>
<td>933</td>
<td>968</td>
<td>3976</td>
<td>132</td>
<td>2312</td>
<td>3976</td>
<td>in.telnetd</td>
</tr>
<tr>
<td>934</td>
<td>968</td>
<td>2140</td>
<td>132</td>
<td>528</td>
<td>2140</td>
<td>oom.sh</td>
</tr>
<tr>
<td>936</td>
<td>173</td>
<td>936</td>
<td>132</td>
<td>132</td>
<td>936</td>
<td>xinetd</td>
</tr>
<tr>
<td>945</td>
<td>968</td>
<td>1472</td>
<td>132</td>
<td>132</td>
<td>1472</td>
<td>libvirtd.sh</td>
</tr>
<tr>
<td>947</td>
<td>592</td>
<td>43164</td>
<td>132</td>
<td>3096</td>
<td>43164</td>
<td>repm</td>
</tr>
<tr>
<td>954</td>
<td>45</td>
<td>932</td>
<td>132</td>
<td>132</td>
<td>932</td>
<td>rpchid</td>
</tr>
<tr>
<td>986</td>
<td>482</td>
<td>3476</td>
<td>132</td>
<td>132</td>
<td>3476</td>
<td>libvirtd</td>
</tr>
<tr>
<td>988</td>
<td>66</td>
<td>940</td>
<td>132</td>
<td>132</td>
<td>940</td>
<td>rpc.statd</td>
</tr>
<tr>
<td>993</td>
<td>968</td>
<td>928</td>
<td>132</td>
<td>928</td>
<td></td>
<td>boothelper_evt.</td>
</tr>
<tr>
<td>1089</td>
<td>102</td>
<td>1200</td>
<td>132</td>
<td>132</td>
<td>1200</td>
<td>rpc.mountd</td>
</tr>
<tr>
<td>1328</td>
<td>9</td>
<td>2940</td>
<td>132</td>
<td>148</td>
<td>2940</td>
<td>rotee</td>
</tr>
<tr>
<td>1353</td>
<td>39</td>
<td>532</td>
<td>132</td>
<td>132</td>
<td>532</td>
<td>sleep</td>
</tr>
</tbody>
</table>

```

The following is a sample output from the `show processes memory platform accounting` command:

```
device# show processes memory platform accounting

Hourly Stats

<table>
<thead>
<tr>
<th>process</th>
<th>callsite_ID(bytes)</th>
<th>max_diff_bytes</th>
<th>callsite_ID(calls)</th>
<th>tracekey</th>
<th>timestamp(UTC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>smand_rp_0</td>
<td>3624155137</td>
<td>172389</td>
<td>3624155138</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>#3a0e4361082c702e5bf1afbd90e6313</td>
<td>2018-09-04 14:23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>linux_iosd-imag_rp_0</td>
<td>3626295305</td>
<td>49188</td>
<td>3624155138</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>#545420bd869d25eb5ab826182ee5d9ce</td>
<td>2018-09-04 12:03</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>btman_rp_0</td>
<td>3624737792</td>
<td>17080</td>
<td>253915394</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>#d6889bd9564a3c4f8f094931ba07a036</td>
<td>2018-09-04 22:29</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fman_fp_image_fp_0</td>
<td>3624059905</td>
<td>16960</td>
<td>4027402242</td>
<td>298</td>
<td></td>
</tr>
<tr>
<td>#921ba4d9df5b0a6e946a3b270bd6592d</td>
<td>2018-09-04 22:55</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following is a sample output from the `show processes memory platform sorted` command:

```
Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches) 277
```

<table>
<thead>
<tr>
<th>Pid</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7885</td>
<td>149848</td>
<td>684864</td>
<td>136</td>
<td>80</td>
<td>684864</td>
<td>linux_iosd-imag</td>
</tr>
<tr>
<td>9655</td>
<td>3787</td>
<td>264964</td>
<td>136</td>
<td>18004</td>
<td>264964</td>
<td>wcm</td>
</tr>
<tr>
<td>17261</td>
<td>324</td>
<td>248588</td>
<td>132</td>
<td>103908</td>
<td>248588</td>
<td>fed main event</td>
</tr>
<tr>
<td>4268</td>
<td>391</td>
<td>102084</td>
<td>136</td>
<td>5596</td>
<td>102084</td>
<td>cli_agent</td>
</tr>
</tbody>
</table>
The following is sample output from the `show processes memory platform sorted location switch active R0` command:

```
device# show processes memory platform sorted location switch active R0
System memory: 3976852K total, 2762884K used, 1213968K free,
Lowest: 1213968K

<table>
<thead>
<tr>
<th>Pid</th>
<th>Text</th>
<th>Data</th>
<th>Stack</th>
<th>Dynamic</th>
<th>RSS</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>7885</td>
<td>149848</td>
<td>684864</td>
<td>136</td>
<td>80</td>
<td>684864</td>
<td>linux_iosd-imag</td>
</tr>
<tr>
<td>9655</td>
<td>3787</td>
<td>264964</td>
<td>136</td>
<td>18004</td>
<td>264964</td>
<td>wcm</td>
</tr>
<tr>
<td>17261</td>
<td>324</td>
<td>248588</td>
<td>132</td>
<td>103908</td>
<td>248588</td>
<td>fed main event</td>
</tr>
<tr>
<td>4268</td>
<td>391</td>
<td>102084</td>
<td>136</td>
<td>5596</td>
<td>102084</td>
<td>cli_agent</td>
</tr>
<tr>
<td>4856</td>
<td>357</td>
<td>93388</td>
<td>132</td>
<td>3680</td>
<td>93388</td>
<td>dbm</td>
</tr>
<tr>
<td>17067</td>
<td>1087</td>
<td>77912</td>
<td>136</td>
<td>1796</td>
<td>77912</td>
<td>platform_mgr</td>
</tr>
</tbody>
</table>

! ! !
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show processes platform

To display information about the IOS-XE processes running on a platform, use the **show processes platform** command in privileged EXEC mode.

```
show processes platform [detailed name process-name] [location switch switch-number | active | standby] {0 | F0 | FP active | R0}
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>detailed</strong></td>
<td>(Optional) Displays detailed information of the specified IOS-XE process.</td>
</tr>
<tr>
<td><strong>name process-name</strong></td>
<td>(Optional) Specifies the process name.</td>
</tr>
<tr>
<td><strong>location</strong></td>
<td>(Optional) Specifies the Field Replaceable Unit (FRU) location.</td>
</tr>
<tr>
<td><strong>switch switch-number</strong></td>
<td>(Optional) Displays information about the switch.</td>
</tr>
<tr>
<td><strong>active</strong></td>
<td>(Optional) Specifies the active instance of the device.</td>
</tr>
<tr>
<td><strong>standby</strong></td>
<td>(Optional) Specifies standby instance of the device.</td>
</tr>
<tr>
<td><strong>0</strong></td>
<td>Specifies the Shared Port Adapter (SPA) Interface Processor slot 0.</td>
</tr>
<tr>
<td><strong>F0</strong></td>
<td>Specifies the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td><strong>FP active</strong></td>
<td>Specifies the active instance in the Embedded Service Processor (ESP).</td>
</tr>
<tr>
<td><strong>R0</strong></td>
<td>Specifies the Route Processor (RP) slot 0.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC(#) | 

**Examples:**

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

```
Device# show processes platform

CPU utilization for five seconds: 1%, one minute: 2%, five minutes: 1%

<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>Status</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>S</td>
<td>4876</td>
<td>systemd</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>S</td>
<td>0</td>
<td>kthreadd</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>ksoftirqd/0</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>kworker/0:0H</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>rcu_sched</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>rcu_bh</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>migration/0</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>watchdog/0</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>watchdog/1</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>S</td>
<td>0</td>
<td>migration/1</td>
</tr>
</tbody>
</table>
```
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pid</td>
<td>Displays the process ID.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Ppid</td>
<td>Displays the process ID of the parent process.</td>
</tr>
<tr>
<td>Status</td>
<td>Displays the process status in human readable form.</td>
</tr>
<tr>
<td>Size</td>
<td>Displays the Resident Set Size (in kilobytes (KB)) that shows how much memory is allocated to that process in the RAM.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the command name associated with the process. Different threads in the same process may have different command values.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cef</td>
<td>(Optional) Displays CEF related information.</td>
</tr>
<tr>
<td>cft</td>
<td>(Optional) Displays CFT related information.</td>
</tr>
<tr>
<td>eigrp</td>
<td>(Optional) Displays EIGRP related information.</td>
</tr>
<tr>
<td>evc</td>
<td>(Optional) Displays EVC related information.</td>
</tr>
<tr>
<td>fnf</td>
<td>(Optional) Displays flexible netflow related information.</td>
</tr>
<tr>
<td>ipc</td>
<td>(Optional) Displays IPC related information.</td>
</tr>
<tr>
<td>ipmulticast</td>
<td>(Optional) Displays IP multicast related information.</td>
</tr>
<tr>
<td>ipsec</td>
<td>(Optional) Displays IPSEC related information.</td>
</tr>
<tr>
<td>mfib</td>
<td>(Optional) Displays MFIB related information.</td>
</tr>
<tr>
<td>nat</td>
<td>(Optional) Displays NAT related information.</td>
</tr>
<tr>
<td>nbar</td>
<td>(Optional) Displays NBAR related information.</td>
</tr>
<tr>
<td>onep</td>
<td>(Optional) Displays ONEP related information.</td>
</tr>
<tr>
<td>ospf</td>
<td>(Optional) Displays OSPF related information.</td>
</tr>
<tr>
<td>page</td>
<td>(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.</td>
</tr>
<tr>
<td>password</td>
<td>(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 &quot;&lt;removed&gt;&quot;.</td>
</tr>
<tr>
<td>rsvp</td>
<td>(Optional) Displays IP RSVP related information.</td>
</tr>
<tr>
<td>subscriber</td>
<td>(Optional) Displays subscriber related information.</td>
</tr>
<tr>
<td>vrrp</td>
<td>(Optional) Displays VRRP related information.</td>
</tr>
<tr>
<td>wccp</td>
<td>(Optional) Displays WCCP related information.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)
### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was implemented.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

You can use one of the following redirection methods:

- `>` `filename` - Redirects the output to a file.
- `>>` `filename` - Redirects the output to a file in append mode.
show tech-support bgp

To automatically run show commands that display BGP related system information, use the `show tech-support bgp` command in the privileged EXEC mode.

```plaintext
show tech-support bgp [address-family {all | ipv4 [flowspec | multicast | unicast | [mdt | mvpn] {all | vrf vrf-instance-name} }] | ipv6 [flowspec | multicast | mvpn {all | vrf vrf-instance-name} | unicast] | l2vpn [evpn | vpls] | link-state [link-state] | [nsap | rtfilter] [unicast] | [vpnv4 | vpnv6] [flowspec | multicast | unicast] {all | vrf vrf-instance-name} | [detail] ]
```

### Syntax Description

- **address-family** (Optional) Displays the output for a specified address family.
- **address-family all** (Optional) Displays the output for all address families.
- **ipv4** (Optional) Displays the output for IPv4 address family.
- **ipv6** (Optional) Displays the output for IPv6 address family.
- **l2vpn** (Optional) Displays the output for L2VPN address family.
- **link-state** (Optional) Displays the output for Link State address family.
- **nsap** (Optional) Displays the output for NSAP address family.
- **rtfilter** (Optional) Displays the output for RT Filter address family.
- **vpnv4** (Optional) Displays the output for VPNv4 address family.
- **vpnv6** (Optional) Displays the output for VPNv6 address family.
- **flowspec** (Optional) Displays the flowspec related information for an address family.
- **multicast** (Optional) Displays the multicast related information for an address family.
- **unicast** (Optional) Displays the unicast related information for an address family.
- **mdt** (Optional) Displays the Multicast Distribution Tree (MDT) related information for an address family.
**show tech-support bgp**

- **mvpn** (Optional) Displays the Multicast VPN (MVPN) related information for an address family.
- **vrf** Displays the information for a VPN Routing/Forwarding instance.
- **evpn** (Optional) Displays the Ethernet VPN (EVPN) related information for an address family.
- **vpls** (Optional) Displays the Virtual Private LAN Services (VPLS) related information for an address family.
- **vrf-instance-name** Specifies the name of the VPN Routing/Forwarding instance.
- **all** Displays the information about all VPN NLRIs.
- **detail** (Optional) Displays the detailed routes information.

**Command Modes**
- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show tech-support bgp` command is used to display the outputs of various BGP show commands and log them to the show-tech file. The output from the `show tech-support bgp` 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.

The following `show` commands run automatically when the `show tech-support bgp` command is used:
- `show clock`
- `show version`
- `show running-config`
- `show process cpu sorted`
- `show process cpu history`
- `show process memory sorted`

The following `show` commands for a specific address family run automatically when the `show tech-support bgp address-family address-family-name address-family-modifier` command is used:
• show bgp address-family-name address-family-modifier summary
• show bgp address-family-name address-family-modifier detail
• show bgp address-family-name address-family-modifier internal
• show bgp address-family-name address-family-modifier neighbors
• show bgp address-family-name address-family-modifier update-group
• show bgp address-family-name address-family-modifier replication
• show bgp address-family-name address-family-modifier community
• show bgp address-family-name address-family-modifier dampening dampened-paths
• show bgp address-family-name address-family-modifier dampening flap-statistics
• show bgp address-family-name address-family-modifier dampening parameters
• show bgp address-family-name address-family-modifier injected-paths
• show bgp address-family-name address-family-modifier cluster-ids
• show bgp address-family-name address-family-modifier cluster-ids internal
• show bgp address-family-name address-family-modifier peer-group
• show bgp address-family-name address-family-modifier pending-prefixes
• show bgp address-family-name address-family-modifier rib-failure

In addition to the above commands, the following segment routing specific show commands also run when the show tech-support bgp command is used:

• show bgp all binding-sid
• show segment-routing client
• show segment-routing mpls state
• show segment-routing mpls gb
• show segment-routing mpls connected-prefix-sid-map protocol ipv4
• show segment-routing mpls connected-prefix-sid-map protocol backup ipv4
• show mpls traffic-eng tunnel auto-tunnel client bgp
show tech-support diagnostic

To display diagnostic information for technical support, use the `show tech-support diagnostic` command in privileged EXEC mode.

**show tech-support diagnostic**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is very long. To better manage this output, you can redirect the output to a file (for example, `show tech-support diagnostic > flash:filename`) in the local writable storage file system or remote file system.

**Note**

For devices that support stacking, this command is executed on every switch that is up. For devices that do not support stacking, this command is executed only on the active switch.

The output of this command displays the output of the following commands:

- show clock
- show version
- show running-config
- show inventory
- show diagnostic bootup level
- show diagnostic status
- show diagnostic content switch all
- show diagnostic result switch all detail
- show diagnostic schedule switch all
- show diagnostic post
- show diagnostic description switch [switch number] test all
- show logging onboard switch [switch number] clilog detail
- show logging onboard switch [switch number] counter detail
- show logging onboard switch [switch number] environment detail
- show logging onboard switch [switch number] message detail
• show logging onboard switch [switch number] poe detail
• show logging onboard switch [switch number] status
• show logging onboard switch [switch number] temperature detail
• show logging onboard switch [switch number] uptime detail
• show logging onboard switch [switch number] voltage detail
show tech-support poe

To display the output of all the PoE-related troubleshooting commands, use the **show tech-support poe** command in privileged EXEC mode. This command displays the output of the following commands:

- `show clock`
- `show version`
- `show running-config`
- `show log`
- `show interface`
- `show interface status`
- `show controllers ethernet-controller`
- `show controllers power inline`
- `show cdp neighbors detail`
- `show lldp neighbors detail`
- `show post`
- `show platform software ilpower details`
- `show platform software ilpower system switch-id`
- `show power inline`
- `show power inline interface-id detail`
- `show power inline police`
- `show power inline priority`
- `show platform software trace message platform-mgr switch switch-number R0`
- `show platform software trace message fed switch switch-number`
- `show platform hardware fed switch switch-number fwd-asic register read register-name pimdeviceid`
- `show platform frontend-controller manager 0 switch-number`
- `show platform frontend-controller subordinate 0 switch-number`
- `show platform frontend-controller version 0 switch-number`
- `show stack-power budgeting`
- `show stack-power detail`

**Command Default**
This command has no arguments or keywords.

**Command Modes**
Privileged EXEC
This example shows the output from the `show tech-support poe` command:

```
Device# show tech-support poe

------------------ show clock ------------------
*17:39:28.741 PDT Wed Aug 22 2018

------------------ show version ------------------
Cisco IOS XE Software, Version Version 16.10.01
Cisco IOS Software [Gibraltar], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.10.1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 13-Jun-18 05:27 by mpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 8.4 DEVELOPMENT SOFTWARE
Switch uptime is 49 minutes
Uptime for this control processor is 53 minutes
System returned to ROM by Image Install
System image file is "flash:packages.conf"
Last reload reason: Image Install

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

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

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

Technology Package License Information:

<table>
<thead>
<tr>
<th>Technology-package</th>
<th>Type</th>
<th>Technology-package</th>
<th>Next reboot</th>
</tr>
</thead>
</table>

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Cisco C9500-12Q (ARM64) processor with 519006K/3071K bytes of memory.
Processor board ID JPG220200A8

1 Virtual Ethernet interface
56 Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
2000996K bytes of physical memory.
819200K bytes of Crash Files at crashinfo:.
819200K bytes of Crash Files at crashinfo-2:.
1941504K bytes of Flash at flash:.
1941504K bytes of Flash at flash-2:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address : 00:bf:77:62:62:80
Motherboard Assembly Number : 73-18700-2
Motherboard Serial Number : JAE220202YB
Model Revision Number : 15
Motherboard Revision Number : 07
Model Number : C9500-12Q
System Serial Number : JPG220200A8

Switch Ports Model       SW Version   SW Image               Mode
--------- ------ -------- -------------- ---------------------
*  1 12   C9500-12Q     16.10.1     CAT9K_LITE_IOSXE       INSTALL

------------------ show running-config ------------------

Building configuration...

Current configuration : 22900 bytes
!
! Last configuration change at 14:59:57 PDT Mon Sep 11 2017
!
version 16.10
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service compress-config
no platform punt-keepalive disable-kernel-core
platform shell
!
hostname stack9-mixed2
!
!
vrf definition Mgmt-vrf
!
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
!
no logging monitor
!
no aaa new-model
boot system switch all flash:packages.conf
!
stack-mac persistent timer 4
switch 1 provision ws-c3850-24xs
!
stack-power stack Powerstack-11
mode redundant strict
!
stack-power switch 1
stack Powerstack-11
!
ip routing
!
crypto pki trustpoint TP-self-signed-2636786964
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-2636786964
revocation-check none
rsakeypair TP-self-signed-2636786964
!
crypto pki certificate chain TP-self-signed-2636786964
certificate self-signed 01

quit
!
errdisable recovery cause inline-power
errdisable recovery interval 30
license boot level ipservicesk9
diagnostic bootup level minimal
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
redundancy
mode sso
!
class-map match-any system-cpp-police-topology-control
description Topology control
class-map match-any system-cpp-police-sw-forward
description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
description EMCL control, EMCL data
!
policy-map port_child_policy
class non-client-nrt-class
bandwidth remaining ratio 10
policy-map system-cpp-policy
  class system-cpp-police-data
    police rate 600 pps
  class system-cpp-police-sys-data
    police rate 100 pps
!
interface Port-channel1
  no switchport
  no ip address
!
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  ip address 10.5.49.131 255.255.255.0
  negotiation auto
!
interface FortyGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/0/1
!
interface FortyGigabitEthernet2/1/1
  shutdown
!
interface TenGigabitEthernet2/1/1
  shutdown
!
interface GigabitEthernet3/0/40
  shutdown
!
interface GigabitEthernet9/0/1
  power inline port poe-ha
!
interface GigabitEthernet9/0/11
  power inline port priority high
!
interface Vlan1
  no ip address
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip tftp source-interface GigabitEthernet0/0
ip route 20.20.20.0 255.255.255.0 2.2.2.3
ip ssh time-out 60
ip ssh authentication-retries 2
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data
  permit tcp any any eq 22
  permit tcp any any eq 465
  permit tcp any any eq 143
  permit tcp any any eq 993
  permit tcp any any eq 995
  permit tcp any any eq 1914
  permit tcp any any eq ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq smtp
  permit tcp any any eq pop3
!
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf
  permit udp any any range 16384 32767
  permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-wlan-Acl-Scavenger
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
permit tcp any any range 6881 6999
permit tcp any any range 28800 29100
permit tcp any any eq 1214
permit udp any any eq 1214
permit tcp any any eq 3689
permit udp any any eq 3689
permit tcp any any eq 11999

ip access-list extended AutoQos-4.0-wlan-Acl-Signaling
permit tcp any any range 2000 2002
permit tcp any any range 5060 5061
permit udp any any range 5060 5061

ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
permit tcp any any eq 443
permit tcp any any eq 1521
permit tcp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
permit tcp any any eq 1527
permit tcp any any eq 6200
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080

control-plane
  service-policy input system-cpp-policy
!
!
no vstack

line con 0
  exec-timeout 0 0
  stopbits 1
  speed 115200
line aux 0
  stopbits 1
line vty 0 4
  login
line vty 5 15
  login
!
mac address-table notification mac-move
wsma agent exec
  profile httplistener
  profile httpplistener
!
wsma agent config
  profile httplistener
  profile httpplistener
!
wsma agent filesys
  profile httplistener
  profile httpplistener
!
wsma agent notify
  profile httplistener
  profile httpplistener
show tech-support poe

wsma profile listener httpListener
  transport http
wsma profile listener httpListener
  transport https
ap dot11 airtime-fairness policy-name Default 0
ap group default-group
ap hyperlocation ble-beacon 0
ap hyperlocation ble-beacon 1
ap hyperlocation ble-beacon 2
ap hyperlocation ble-beacon 3
ap hyperlocation ble-beacon 4
end

------------------ show log ------------------

Syslog logging: enabled (0 messages dropped, 16 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

Console logging: disabled
Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled
Buffer logging: level debugging, 782 messages logged, xml disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
File logging: disabled
Persistent logging: disabled

No active filter modules.
Trap logging: level informational, 310 message lines logged

Logging Source-Interface: VRF Name:

Log Buffer (4096 bytes):

Aug 22 17:17:28.966 PDT: %LINK-3-UPDOWN: Interface FortyGigabitEthernet1/0/1, changed state to down

Aug 22 17:17:29.196 PDT: %ILPOWER-5-POWER_GRANTED: Interface Fo1/0/1: Power granted

Aug 22 17:17:47.209 PDT: %SYS-5-CONFIG_I: Configured from console by console

Aug 22 17:17:50.200 PDT: %ILPOWER-7-DETECT: Interface Fo1/0/1: Power Device detected: IEEE PD

Aug 22 17:17:51.822 PDT: %ILPOWER-5-POWER_GRANTED: Interface Fo1/0/1: Power granted

Aug 22 17:17:52.321 PDT: ilpower delete power from pd linkdown Fo1/0/1

Aug 22 17:17:52.321 PDT: Ilpower interface (Fo1/0/1), delete allocated power 15400

Aug 22 17:17:52.321 PDT: Ilpower interface (Fo1/0/1), setting ICUT_OFF threshold to 0.

Aug 22 17:17:52.321 PDT: ilpower_notify_lldp_power_via_mdi_tlv Fo1/0/1 pwr alloc 0

Aug 22 17:17:52.321 PDT: Fo1/0/1 AUTO PORT PWR Alloc 130 Request 130

Aug 22 17:17:52.321 PDT: ILP notify LLDB-TLV: lldp power class tlv:

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Aug 22 17:17:52.321 PDT: (curr/prev) pwr value 15400/0
Aug 22 17:17:52.322 PDT: %SYS-5-CONFIG_I: Configured from console by console
Aug 22 17:17:54.323 PDT: %LINK-5-CHANGED: Interface FiveGigabitEthernet1/0/1, changed state to administratively down
Aug 22 17:18:11.981 PDT: ILP notify LLDB-TLV: lldp power class tlv:
Aug 22 17:18:11.981 PDT: (curr/prev) pwr value 15400/0
Aug 22 17:18:11.982 PDT: %SYS-5-CONFIG_I: Configured from console by console
Aug 22 17:18:13.207 PDT: (Fo1/0/1) data power pool 1
Aug 22 17:18:13.207 PDT: Ilpower PD device 3 class 6 from interface (Fo1/0/1)
Aug 22 17:18:13.207 PDT: (Fo1/0/1) state auto
Aug 22 17:18:13.207 PDT: (Fo1/0/1) data power pool: 1, pool 1
Aug 22 17:18:13.207 PDT: (Fo1/0/1) curr pwr usage 15400
Aug 22 17:18:13.207 PDT: (Fo1/0/1) req pwr 15400
Aug 22 17:18:13.207 PDT: (Fo1/0/1) total pwr 610000
Aug 22 17:18:13.207 PDT: (Fo1/0/1) power_status OK
Aug 22 17:18:13.207 PDT: ilpower new power from pd discovery Fo1/0/1, power_status ok
Aug 22 17:18:13.207 PDT: Ilpower interface (Fo1/0/1) power status change, allocated power 15400
Aug 22 17:18:13.207 PDT: ILP notify LLDB-TLV: lldp power class tlv:
Aug 22 17:18:13.207 PDT: (curr/prev) pwr value 15400/0
Aug 22 17:18:13.207 PDT: ilpower_notify_lldp_power_via_mdi_tlv Fo1/0/1 pwr alloc 15400
Aug 22 17:18:13.208 PDT: Fo1/0/1 AUTO PORT PWR Alloc 130 Request 130
Aug 22 17:18:13.208 PDT: Fo1/0/1: LLDP NOTIFY TLV:
   (curr/prev) PSE Allocation (mW): 13000/0
   (curr/prev) PD Request (mW) : 13000/0
   (curr/prev) PD Class : Class 3/
   (curr/prev) PD Priority : low/unknown
   (curr/prev) Power Type : Type 2 PSE/Type 2 PSE
   (curr/prev) mdi_pwr_support: 15/0
   (curr/prev) Power Pair : Signal/
   (curr/prev) PSE Pwr Source : Primary/Unknown
Aug 22 17:18:13.981 PDT: %LINK-3-UPDOWN: Interface FoveGigabitEthernet1/0/1, changed state to down

Aug 22 17:18:14.207 PDT: %ILPOWER-5-POWER_GRANTED: Interface Fo1/0/1: Power granted

Aug 22 17:18:32.180 PDT: %SYS-5-LOG_CONFIG_CHANGE: Console logging disabled

Aug 22 17:18:32.242 PDT: %SYS-5-CONFIG_I: Configured from console by console

Aug 22 17:47:45.133 PDT: %SYS-5-CONFIG_I: Configured from console by console

Aug 22 17:47:45.717 PDT: %SYS-5-CONFIG_I: Configured from console by console

Aug 22 17:47:45.000 PDT: %SYS-6-CLOCKUPDATE: System clock has been updated from 17:47:45 PDT Wed Aug 22 2018 to 17:47:45 PDT Wed Aug 22 2018, configured from console by console.

------------------ show controllers power inline module 1 ------------------

Alchemy instance 0, address 0

Pending event flag : N N N N N N N N N N N N
Current State : 00 00 10 93 D8 E8
Current Event : 11 11 14 00 00 00
Timers : 22 00 00 00 00 00 00 00 00 00 00 00
Error State : 14 14 14 14 14 14
Error Code : 00 00 00 00 00 00 00 00 00 00 00 00
Power Status : N N N N N N N N N N N
Auto Config : N N N N N N N N N N N N
Disconnect : N N N N N N N N N N N N
Detection Status : F0 00 10 00 00 00
Current Class : 00 00 00 00 00 00
Tweetie debug : 00 00 00 00
POE Commands pending at sub:
  Command 0 on each port : 00 00 00 00 00 00
  Command 1 on each port : 00 00 00 00 00 00
  Command 2 on each port : 00 00 00 00 00 00
  Command 3 on each port : 00 00 00 00 00 00

Alchemy instance 1, address E

Pending event flag : N N N N N N N N N N N N
Current State : 00 00 10 93 D8 E8
Current Event : 11 11 14 00 00 00
Timers : 2A 00 00 00 00 00 00 00 00 00 00 00
Error State : 26 26 26 26 26 26 2A
Error Code : 00 00 00 00 00 00 00 00 00 00 00 00
Power Status : N N N N N N N N N N N N
Auto Config : N N N N N N N N N N N N
Disconnect : N N N N N N N N N N N N
Detection Status : F0 00 00 00 00 00
Current Class : 00 00 00 00 00 00
Tweetie debug : 00 00 00 00
POE Commands pending at sub:
  Command 0 on each port : 00 00 00 00 00 00
  Command 1 on each port : 00 00 00 00 00 00
  Command 2 on each port : 00 00 00 00 00 00
  Command 3 on each port : 00 00 00 00 00 00

------------------ show platform software ilpower details ------------------

ILP Port Configuration for interface Te2/0/1
Initialization Done: Yes
ILP Supported: Yes
ILP Enabled: Yes
POST: Yes
Detect On: No
Powered Device Detected: Yes
Powered Device Class Done: No
Cisco Powered Device: No
Power is On: No
Power Denied: No
Powered Device Type: Null
Powered Device Class: Null
Power State: Off
Current State: NGWC_ILP_DETECTING_S
Previous State: NGWC_ILP_DETECTING_S
Requested Power in milli watts: 0
Short Circuit Detected: 0
Short Circuit Count: 0
Cisco Powered Device Detect Count: 0
Spare Pair mode: 0
Spare Pair Architecture: 1
Signal Pair Power allocation in milli watts: 0
Spare Pair Power On: 0
Powered Device power state: 0
Timer:
  Power Good: Stopped
  Power Denied: Stopped
  Cisco Powered Device Detect: Stopped
  IEEE Detect: Stopped
  IEEE Short: Stopped
  Link Down: Stopped
  Voltage sense: Stopped

------------------ show platform software ilpower system 3 ------------------

ILP System Configuration
Slot: 3
ILP Supported: Yes
Total Power: 1101000
Used Power: 49400
Initialization Done: Yes
Post Done: Yes
Post Result Logged: No
Post Result: Success
Power Summary:
  Module: 0
  Power Total: 1101000
  Power Used: 49400
  Power Threshold: 0
  Operation Status: On
Pool: 3
Pool Valid: Yes
Total Power: 1101000
Power Usage: 49400

------------------ show power inline Gi9/0/16 detail ------------------

Interface: Gi9/0/16
Inline Power Mode: auto
Operational status: off
Device Detected: no
Device Type: n/a
IEEE Class: n/a
Discovery mechanism used/configured: Ieee and Cisco

Police: off

Power Allocated
Admin Value: 60.0
Power drawn from the source: 0.0
Power available to the device: 0.0

Actual consumption
Measured at the port: 0.0
Maximum Power drawn by the device since powered on: 0.0

Absent Counter: 0
Over Current Counter: 0
Short Current Counter: 0
Mosfet Counter: 0
Invalid Signature Counter: 0
Power Denied Counter: 0

Power Negotiation Used: None
LLDP Power Negotiation --Sent to PD-- --Rcvd from PD--
Power Type: - -
Power Source: - -
Power Priority: - -
Requested Power (W): - -
Allocated Power (W): - -

Four-Pair PoE Supported: Yes
Spare Pair Power Enabled: No
Four-Pair PD Architecture: N/A

------------------ show power inline Te8/0/1 detail ------------------

Interface Te8/0/1: inline power not supported

------------------ show power inline police ------------------

<table>
<thead>
<tr>
<th>Module</th>
<th>Available (Watts)</th>
<th>Used (Watts)</th>
<th>Remaining (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Admin Power</th>
<th>Oper Power</th>
<th>Cutoff Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te2/0/1</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/2</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/3</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/4</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/5</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/6</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>

Totals: 0.0

<table>
<thead>
<tr>
<th>Module</th>
<th>Available (Watts)</th>
<th>Used (Watts)</th>
<th>Remaining (Watts)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1050.0</td>
<td>0.0</td>
<td>1050.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Admin Power</th>
<th>Oper Power</th>
<th>Cutoff Power</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te2/0/1</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/2</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/3</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/4</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/5</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Te2/0/6</td>
<td>auto</td>
<td>off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
</tr>
</tbody>
</table>
### Interface and Hardware Components

#### show tech-support poe

<table>
<thead>
<tr>
<th>Interface</th>
<th>Admin State</th>
<th>Oper State</th>
<th>Admin Oper Power</th>
<th>Oper Power</th>
<th>Cutoff Power</th>
<th>Oper Cutoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi3/0/1</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/2</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/3</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/4</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/5</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/6</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/7</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/8</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/9</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/10</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/11</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/12</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/13</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>3.6</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/14</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>7.0</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/15</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/16</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>3.7</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/17</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>3.7</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/18</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/19</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>3.7</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/20</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/21</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>3.7</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/22</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/23</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/24</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/25</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/26</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/27</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/28</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/29</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/30</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/31</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/32</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/33</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/34</td>
<td>auto off</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Gi3/0/35</td>
<td>auto on</td>
<td>none</td>
<td>n/a</td>
<td>n/a</td>
<td>2.3</td>
<td>n/a</td>
</tr>
</tbody>
</table>

---

Totsals: 0.0

**Module** | **Available (Watts)** | **Used (Watts)** | **Remaining (Watts)**
--- | --- | --- | ---
3 | 1131.0 | 49.4 | 1081.6

---

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**

302
show tech-support poe

showing manager info: 1

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show tech-support poe

Tx cmd cnt POE_E App -369383984
Rx cmd cnt POE_E App -369346528
Tx cmd ignore POE_E App -1826379312
Tx cmd Q full POE_E App -394693324
Tx cmd cnt DMSG App 0
Rx cmd cnt DMSG App 0
Tx cmd ignore DMSG App 0
Tx cmd Q full DMSG App 255
Tx reg cnt 16
Rx reg cnt 16
Tx reg ignore 0
Tx reg Q full 0
Rx invalid frame 0
Rx invalid App 748
Rx invalid Seq 0
Rx invalid checksum 0
Nack cnt 0
Send Break count 0
Early Send Break count 0
Retransmission cnt 0

------------------ show platform frontend-controller subordinate 0 1 ------------------

  showing sub info: 1
  State OK
  Last Reset Reason UNKNOWN REASON
  UART FE Error 0
  UART PE Error 0
  UART DOR Error 0
  Rx Buf Overflow 0
  Rx Buf Underflow 0
  Tx Buf Full 0
  Rx Bad Endbyte 0
  PLE Invalid App 0
  PLE Disabled App 0
  PLE Invalid Data 0
  PLE Invalid Flags 0
  PLE Invalid Reg 0
  PLE Invalid Reg Len 0
  PLE Invalid Mag Len 0
  SLE Poe No Port 0
  SLE I2C Busy 0
  SLE I2C Error 0
  SLE I2C Timeout 0
  SLE Invalid Reg Len 0
  SLE Msg Underrun 0

------------------ show platform frontend-controller version 0 1 ------------------

Switch 1 MCU:
  Software Version 0.109
  System Type 6
  Device Id 2
  Device Revision 0
  Hardware Version 41
  Bootloader Version 16
**speed**

To specify the speed of a port, use the `speed` command in interface configuration mode. To return to the default value, use the `no` form of this command.

**Note**

Available configuration options depend on the switch model and transceiver module installed. Options include 10, 100, 1000, 2500, 5000, 10000, 25000, 40000, 100000

```plaintext
speed {10 | 100 | 1000 | 2500 | 5000 | 10000 | 25000 | 40000 | 100000 | 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.
- **10000** Specifies that the port runs at 10000 Mbps operation.
- **25000** Specifies that the port runs at 25000 Mbps operation.
- **40000** Specifies that the port runs at 40000 Mbps operation.
- **100000** Specifies that the port runs at 100000 Mbps operation.
- **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, 10000, 25000, or 50000** 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 (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.2</td>
<td>Support for 10000 and 25000 Mbps options with dual-rate transceivers was introduced.</td>
</tr>
</tbody>
</table>
Modification
Support for 40000 and 100000 Mbps options with dual-rate transceivers was introduced.

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.

When you install dual-rate transceiver modules (on supported switch models), entering the the speed command displays the dual configuration options that are available with the transceiver module. For information about such transceiver modules and device compatibility, see: the Transceiver Module Group (TMG) Compatibility Matrix.

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
```
**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}
o switchport block {multicast | unicast}
```

**Syntax Description**
- `multicast` Specifies that unknown multicast traffic should be blocked.
  
  **Note**: Only pure Layer 2 multicast traffic is blocked. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

- `unicast` Specifies that unknown unicast traffic should be blocked.

**Command Default**
Unknown multicast and unicast traffic is not blocked.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

With multicast traffic, the port blocking feature blocks only pure Layer 2 packets. Multicast packets that contain IPv4 or IPv6 information in the header are not blocked.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

For more information about blocking packets, see the software configuration guide for this release.

This example shows how to block unknown unicast traffic on an interface:

```
Device(config-if)# switchport block unicast
```

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

To set the global maximum packet size or MTU size for switched packets on Gigabit Ethernet and 10-Gigabit Ethernet ports, use the `system mtu` command in global configuration mode. To restore the global MTU value to its default value, use the `no` form of this command.

```
system mtu  bytes
no system mtu
```

**Syntax Description**
- `bytes` The global MTU size in bytes. The range is 1500 to 9198 bytes; the default is 1500 bytes.

**Command Default**
The default MTU size for all ports is 1500 bytes.

**Command Modes**
- Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
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

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

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

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

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

These profile attributes are contained in the Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) network-policy time-length-value (TLV).
To return to privileged EXEC mode from the network-policy profile configuration mode, enter the `exit` command.

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

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

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

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

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

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

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

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

Syntax Description

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

Command Default

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

- The default CoS value is 5.
- The default DSCP value is 46.
- The default tagging mode is untagged.

Command Modes

Network-policy profile configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 IV

IP Addressing Services

- IP Addressing Services Commands, on page 315
IP Addressing Services Commands

• clear ip nhrp, on page 320
• clear ipv6 access-list, on page 321
• clear ipv6 dhcp, on page 322
• clear ipv6 dhcp binding, on page 323
• clear ipv6 dhcp client, on page 324
• clear ipv6 dhcp conflict, on page 325
• clear ipv6 dhcp relay binding, on page 326
• clear ipv6 eigrp, on page 327
• clear ipv6 mfib counters, on page 328
• clear ipv6 mld counters, on page 329
• clear ipv6 mld traffic, on page 330
• clear ipv6 mtu, on page 331
• clear ipv6 multicast aaa authorization, on page 332
• clear ipv6 nd destination, on page 333
• clear ipv6 nd on-link prefix, on page 334
• clear ipv6 nd router, on page 335
• clear ipv6 neighbors, on page 336
• clear ipv6 nhrp, on page 338
• clear ipv6 ospf, on page 339
• clear ipv6 ospf counters, on page 340
• clear ipv6 ospf events, on page 342
• clear ipv6 pim reset, on page 343
• clear ipv6 pim topology, on page 344
• clear ipv6 pim traffic, on page 345
• clear ipv6 prefix-list, on page 346
• clear ipv6 rip, on page 347
• clear ipv6 route, on page 348
• clear ipv6 spd, on page 349
• debug nhrp, on page 350
• fhrp delay, on page 352
• fhrp version vrrp v3, on page 353
• ip address dhcp, on page 354
• ip address pool (DHCP), on page 357
• ip address, on page 358
• ip nhrp authentication, on page 361
• ip nhrp holdtime, on page 362
• ip nhrp map, on page 363
• ip nhrp map multicast, on page 365
• ip nhrp network-id, on page 366
• ip nhrp nhs, on page 367
• ip nhrp registration, on page 369
• ipv6 access-list, on page 370
• ipv6 address-validate, on page 373
• ipv6 cef, on page 374
• ipv6 cef accounting, on page 376
• ipv6 cef distributed, on page 378
• ipv6 cef load-sharing algorithm, on page 380
• ipv6 cef optimize neighbor resolution, on page 381
• ipv6 destination-guard policy, on page 382
• ipv6 dhcp-relay bulk-lease, on page 383
• ipv6 dhcp-relay option vpn, on page 384
• ipv6 dhcp-relay source-interface, on page 385
• ipv6 dhcp binding track ppp, on page 386
• ipv6 dhcp database, on page 387
• ipv6 dhcp iana-route-add, on page 389
• ipv6 dhcp iapd-route-add, on page 390
  • ipv6 dhcp-ldra, on page 391
• ipv6 dhcp ping packets, on page 392
• ipv6 dhcp pool, on page 393
• ipv6 dhcp server vrf enable, on page 395
• ipv6 flow monitor, on page 396
• ipv6 general-prefix, on page 397
• ipv6 local policy route-map, on page 399
• ipv6 local pool, on page 401
• ipv6 mld snooping, on page 403
• ipv6 mld ssm-map enable, on page 404
• ipv6 mld state-limit, on page 405
• ipv6 multicast-routing, on page 406
• ipv6 multicast group-range, on page 407
• ipv6 multicast pim-passive-enable, on page 409
• ipv6 multicast rpf, on page 410
• ipv6 nd cache expire, on page 411
• ipv6 nd cache interface-limit (global), on page 412
• ipv6 nd host mode strict, on page 413
• ipv6 nd na glean, on page 414
• ipv6 nd ns-interval, on page 415
• ipv6 nd nud retry, on page 416
• ipv6 nd reachable-time, on page 418
• ipv6 nd resolution data limit, on page 419
• show ipv6 mtu, on page 509
• show ipv6 nd destination, on page 511
• show ipv6 nd on-link prefix, on page 512
• show ipv6 neighbors, on page 513
• show ipv6 nhrp, on page 517
• show ipv6 ospf, on page 520
• show ipv6 ospf border-routers, on page 524
• show ipv6 ospf event, on page 526
• show ipv6 ospf graceful-restart, on page 529
• show ipv6 ospf interface, on page 531
• show ipv6 ospf request-list, on page 536
• show ipv6 ospf retransmission-list, on page 538
• show ipv6 ospf statistics, on page 540
• show ipv6 ospf summary-prefix, on page 542
• show ipv6 ospf timers rate-limit, on page 543
• show ipv6 ospf traffic, on page 544
• show ipv6 ospf virtual-links, on page 548
• show ipv6 pim anycast-RP, on page 550
• show ipv6 pim bsr, on page 551
• show ipv6 pim df, on page 553
• show ipv6 pim group-map, on page 555
• show ipv6 pim interface, on page 557
• show ipv6 pim join-prune statistic, on page 559
• show ipv6 pim limit, on page 560
• show ipv6 pim neighbor, on page 561
• show ipv6 pim range-list, on page 563
• show ipv6 pim topology, on page 565
• show ipv6 pim traffic, on page 567
• show ipv6 pim tunnel, on page 569
• show ipv6 policy, on page 571
• show ipv6 prefix-list, on page 572
• show ipv6 protocols, on page 575
• show ipv6 rip, on page 578
• show ipv6 route, on page 583
• show ipv6 routers, on page 587
• show ipv6 rpf, on page 590
• show ipv6 source-guard policy, on page 592
• show ipv6 spd, on page 593
• show ipv6 static, on page 594
• show ipv6 traffic, on page 598
• show key chain, on page 601
• show track, on page 602
• track, on page 604
• vrrp, on page 606
• vrrp description, on page 607
• vrrp preempt, on page 608
• vrrp priority, on page 609
• vrrp timers advertise, on page 610
• vrrs leader, on page 612
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**
- **vrf** (Optional) Deletes entries from the NHRP cache for the specified virtual routing and forwarding (VRF) instance.
- **vrf-name** (Optional) Name of the VRF address family to which the command is applied.
- **global** (Optional) Specifies the global VRF instance.
- **dest-ip-address** (Optional) Destination IP address. Specifying this argument clears NHRP mapping entries for the specified destination IP address.
- **dest-mask** (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**
- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip nhrp</td>
<td>Displays NHRP mapping information.</td>
</tr>
</tbody>
</table>
clear ipv6 access-list

To reset the IPv6 access list match counters, use the `clear ipv6 access-list` command in privileged EXEC mode.

```plaintext
clear ipv6 access-list [access-list-name]
```

**Syntax Description**

| access-list-name | (Optional) Name of the IPv6 access list for which to clear the match counters. Names cannot contain a space or quotation mark, or begin with a numeric. |

**Command Default**

No reset is initiated.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear ipv6 access-list` command is similar to the `clear ip access-list counters` command, except that it is IPv6-specific.

The `clear ipv6 access-list` command used without the `access-list-name` argument resets the match counters for all IPv6 access lists configured on the router.

This command resets the IPv6 global ACL hardware counters.

**Examples**

The following example resets the match counters for the IPv6 access list named marketing:

```plaintext
Device# clear ipv6 access-list marketing
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware statistics</td>
<td>Enables the collection of hardware statistics.</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>Defines an IPv6 access list and enters IPv6 access list configuration mode.</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>Displays the contents of all current IPv6 access lists.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcp

To clear IPv6 Dynamic Host Configuration Protocol (DHCP) information, use the clear ipv6 dhcp command in privileged EXEC mode:

```
clear ipv6 dhcp
```

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

### Command Modes
Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
The clear ipv6 dhcp command deletes DHCP for IPv6 information.

### Examples
The following example:

```
Device# clear ipv6 dhcp
```
clear ipv6 dhcp binding

To delete automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the `clear ipv6 dhcp binding` command in privileged EXEC mode.

```
clear ipv6 dhcp binding [ipv6-address] [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>(Optional) The address of a DHCP for IPv6 client. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear ipv6 dhcp binding` command is used as a server function.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes’ valid lifetimes have expired, or an administrator runs the `clear ipv6 dhcp binding` command.

If the `clear ipv6 dhcp binding` command is used with the optional `ipv6-address` argument specified, only the binding for the specified client is deleted. If the `clear ipv6 dhcp binding` command is used without the `ipv6-address` argument, then all automatic client bindings are deleted from the DHCP for IPv6 binding table. If the optional `vrf vrf-name` keyword and argument combination is used, only the bindings for the specified VRF are cleared.

**Examples**

The following example deletes all automatic client bindings from the DHCP for IPv6 server binding table:

```
Device# clear ipv6 dhcp binding
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcp binding</td>
<td>Displays automatic client bindings from the DHCP for IPv6 server binding table.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcp client

To restart the Dynamic Host Configuration Protocol (DHCP) for IPv6 client on an interface, use the `clear ipv6 dhcp client` command in privileged EXEC mode.

`clear ipv6 dhcp client interface-type interface-number`

**Syntax Description**

| interface-type interface-number | Interface type and number. For more information, use the question mark (?) online help function. |

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `clear ipv6 dhcp client` command restarts the DHCP for IPv6 client on specified interface after first releasing and unconfiguring previously acquired prefixes and other configuration options (for example, Domain Name System [DNS] servers).

**Examples**

The following example restarts the DHCP for IPv6 client for Ethernet interface 1/0:

```
Device# clear ipv6 dhcp client Ethernet 1/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 dhcp interface</code></td>
<td>Displays DHCP for IPv6 interface information.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcp conflict

To clear an address conflict from the Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server database, use the `clear ipv6 dhcp conflict` command in privileged EXEC mode.

```
clear ipv6 dhcp conflict {* | ipv6-address | vrf vrf-name}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Clears all address conflicts.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>Clears the host IPv6 address that contains the conflicting address.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Specifies a virtual routing and forwarding (VRF) name.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

If you use the asterisk (*) character as the address parameter, DHCP clears all conflicts.

If the `vrf vrf-name` keyword and argument are specified, only the address conflicts that belong to the specified VRF will be cleared.

### Examples

The following example shows how to clear all address conflicts from the DHCPv6 server database:

```
Device# clear ipv6 dhcp conflict *
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcp conflict</td>
<td>Displays address conflicts found by a DHCPv6 server when addresses are offered to the client.</td>
</tr>
</tbody>
</table>
clear ipv6 dhcp relay binding

To clear an IPv6 address or IPv6 prefix of a Dynamic Host Configuration Protocol (DHCP) for IPv6 relay binding, use the **clear ipv6 dhcp relay binding** command in privileged EXEC mode.

`clear ipv6 dhcp relay binding {vrf vrf-name} {* ipv6-address ipv6-prefix}`

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>*</td>
<td>Clears all DHCPv6 relay bindings.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>DHCPv6 address.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>IPv6 prefix.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **clear ipv6 dhcp relay binding** command deletes a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding. If no relay client is specified, no binding is deleted.

### Examples

The following example shows how to clear the binding for a client with a specified IPv6 address:

```
Device# clear ipv6 dhcp relay binding 2001:0DB8:3333:4::5
```

The following example shows how to clear the binding for a client with the VRF name vrf1 and a specified prefix on a Cisco uBR10012 universal broadband device:

```
Device# clear ipv6 dhcp relay binding vrf vrf1 2001:DB8::1::/64
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 dhcp relay binding</td>
<td>Displays DHCPv6 IANA and DHCPv6 IAPD bindings on a relay agent.</td>
</tr>
</tbody>
</table>
clear ipv6 eigrp

To delete entries from Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 routing tables, use the `clear ipv6 eigrp` command in privileged EXEC mode.

```
clear ipv6 eigrp [as-number] [neighbor [ipv6-address | interface-type interface-number]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>(Optional) Autonomous system number.</td>
</tr>
<tr>
<td><code>neighbor</code></td>
<td>(Optional) Deletes neighbor router entries.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>(Optional) IPv6 address of a neighboring router.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) The interface type of the neighbor router.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>(Optional) The interface number of the neighbor router.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `clear ipv6 eigrp` command without any arguments or keywords to clear all EIGRP for IPv6 routing table entries. Use the `as-number` argument to clear routing table entries on a specified process, and use the `neighbor/ipv6-address` keyword and argument, or the `interface-type interface-number` argument, to remove a specific neighbor from the neighbor table.

### Examples

The following example removes the neighbor whose IPv6 address is 3FEE:12E1:2AC1:EA32:

```
Device# clear ipv6 eigrp neighbor 3FEE:12E1:2AC1:EA32
```
clear ipv6 mfib counters

To reset all active Multicast Forwarding Information Base (MFIB) traffic counters, use the `clear ipv6 mfib counters` command in privileged EXEC mode.

```
clear ipv6 mfib [vrf vrf-name] counters [{group-name | group-address [{source-address source-name}]}]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a virtual routing and forwarding (VRF) configuration.
- **group-name | group-address** (Optional) IPv6 address or name of the multicast group.
- **source-address | source-name** (Optional) IPv6 address or name of the source.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

After you enable the `clear ipv6 mfib counters` command, you can determine if additional traffic is forwarded by using one of the following show commands that display traffic counters:

- `show ipv6 mfib`
- `show ipv6 mfib active`
- `show ipv6 mfib count`
- `show ipv6 mfib interface`
- `show ipv6 mfib summary`

**Examples**

The following example clears and resets all MFIB traffic counters:

```
Device# clear ipv6 mfib counters
```
clear ipv6 mld counters

To clear the Multicast Listener Discovery (MLD) interface counters, use the `clear ipv6 mld counters` command in privileged EXEC mode.

```
clear ipv6 mld [vrf vrf-name] counters [interface-type]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `clear ipv6 mld counters` command to clear the MLD counters, which keep track of the number of joins and leaves received. If you omit the optional `interface-type` argument, the `clear ipv6 mld counters` command clears the counters on all interfaces.

**Examples**

The following example clears the counters for Ethernet interface 1/0:

```
Device# clear ipv6 mld counters Ethernet1/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld interface</td>
<td>Displays multicast-related information about an interface.</td>
</tr>
</tbody>
</table>
clear ipv6 mld traffic

To reset the Multicast Listener Discovery (MLD) traffic counters, use the **clear ipv6 mld traffic** command in privileged EXEC mode.

```
clear ipv6 mld [vrf vrf-name] traffic
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using the **clear ipv6 mld traffic** command will reset all MLD traffic counters.

**Examples**

The following example resets the MLD traffic counters:

```
Device# clear ipv6 mld traffic
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mld traffic</td>
<td>Displays the MLD traffic counters.</td>
</tr>
</tbody>
</table>
clear ipv6 mtu

To clear the maximum transmission unit (MTU) cache of messages, use the `clear ipv6 mtu` command in privileged EXEC mode.

**clear ipv6 mtu**

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

### Command Default
Messages are not cleared from the MTU cache.

### Command Modes
Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
If a router is flooded with ICMPv6 too big messages, the router is forced to create an unlimited number of entries in the MTU cache until all available memory is consumed. Use the `clear ipv6 mtu` command to clear messages from the MTU cache.

### Examples
The following example clears the MTU cache of messages:

```
Device# clear ipv6 mtu
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 flowset</td>
<td>Configures flow-label marking in 1280-byte or larger packets sent by the router.</td>
</tr>
</tbody>
</table>
clear ipv6 multicast aaa authorization

To clear authorization parameters that restrict user access to an IPv6 multicast network, use the `clear ipv6 multicast aaa authorization` command in privileged EXEC mode.

```
clear ipv6 multicast aaa authorization [interface-type interface-number]
```

**Syntax Description**

- `interface-type interface-number` Interface type and number. For more information, use the question mark (”) online help function.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using the `clear ipv6 multicast aaa authorization` command without the optional `interface-type` and `interface-number` arguments will clear all authorization parameters on a network.

**Examples**

The following example clears all configured authorization parameters on an IPv6 network:

```
Device# clear ipv6 multicast aaa authorization FastEthernet 1/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa authorization multicast default</td>
<td>Sets parameters that restrict user access to an IPv6 multicast network.</td>
</tr>
</tbody>
</table>
clear ipv6 nd destination

To clear IPv6 host-mode destination cache entries, use the clear ipv6 nd destination command in privileged EXEC mode.

clear ipv6 nd destination[vrf vrf-name]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The clear ipv6 nd destination command clears IPv6 host-mode destination cache entries. If the vrf vrf-name keyword and argument pair is used, then only information about the specified VRF is cleared.

Examples

The following example shows how to clear IPv6 host-mode destination cache entries:

```
Device# clear ipv6 nd destination
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd host mode strict</td>
<td>Enables the conformant, or strict, IPv6 host mode.</td>
</tr>
</tbody>
</table>
# clear ipv6 nd on-link prefix

To clear on-link prefixes learned through router advertisements (RAs), use the `clear ipv6 nd on-link prefix` command in privileged EXEC mode.

```
clear ipv6 nd on-link prefix[vrf vrf-name]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
</tbody>
</table>

## Command Modes

Privileged EXEC (#)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the `clear ipv6 nd on-link prefix` command to clear locally reachable IPv6 addresses (e.g., on-link prefixes) learned through RAs. If the `vrf vrf-name` keyword and argument pair is used, then only information about the specified VRF is cleared.

## Examples

The following examples shows how to clear on-link prefixes learned through RAs:

```
Device# clear ipv6 nd on-link prefix
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd host mode strict</td>
<td>Enables the conformant, or strict, IPv6 host mode.</td>
</tr>
</tbody>
</table>
clear ipv6 nd router

To clear neighbor discovery (ND) device entries learned through router advertisements (RAs), use the clear ipv6 nd router command in privileged EXEC mode.

```
clear ipv6 nd router[vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>vrf vrf-name</th>
<th>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</th>
</tr>
</thead>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `clear ipv6 nd router` command to clear ND device entries learned through RAs. If the `vrf vrf-name` keyword and argument pair is used, then only information about the specified VRF is cleared.

**Examples**

The following example shows how to clear neighbor discovery ND device entries learned through RAs:

```
Device# clear ipv6 nd router
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd host mode strict</td>
<td>Enables the conformant, or strict, IPv6 host mode.</td>
</tr>
</tbody>
</table>
clear ipv6 neighbors

To delete all entries in the IPv6 neighbor discovery cache, except static entries and ND cache entries on non-virtual routing and forwarding (VRF) interfaces, use the **clear ipv6 neighbors** command in privileged EXEC mode.

```
clear ipv6 neighbors [{interface type number[ipv6 ipv6-address] | statistics | vrf table-name [{ipv6-address | statistics}]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type number</td>
<td>(Optional) Clears the IPv6 neighbor discovery cache in the specified interface.</td>
</tr>
<tr>
<td>ipv6 ipv6-address</td>
<td>(Optional) Clears the IPv6 neighbor discovery cache that matches the specified IPv6 address on the specified interface.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Clears the IPv6 neighbor discovery entry cache.</td>
</tr>
<tr>
<td>vrf table-name</td>
<td>(Optional) Clears entries for a virtual private network (VPN) routing or forwarding instance.</td>
</tr>
<tr>
<td>table-name</td>
<td>(Optional) Table name or identifier. The value range is from 0x0 to 0xFFFFFFFF (0 to 65535 in decimal).</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **clear ipv6 neighbors** command clears ND cache entries. If the command is issued without the **vrf** keyword, then the command clears ND cache entries on interfaces associated with the default routing table (e.g., those interfaces that do not have a **vrf forwarding** statement). If the command is issued with the **vrf** keyword, then it clears ND cache entries on interfaces associated with the specified VRF.

### Examples

The following example deletes all entries, except static entries and ND cache entries on non-VRF interfaces, in the neighbor discovery cache:

```
Device# clear ipv6 neighbors
```

The following example clears all IPv6 neighbor discovery cache entries, except static entries and ND cache entries on non-VRF interfaces, on Ethernet interface 0/0:

```
Device# clear ipv6 neighbors interface Ethernet 0/0
```

The following example clears a neighbor discovery cache entry for 2001:0DB8:1::1 on Ethernet interface 0/0:

```
Device# clear ipv6 neighbors address 2001:0DB8:1::1
```
In the following example, interface Ethernet 0/0 is associated with the VRF named red. Interfaces Ethernet 1/0 and Ethernet 2/0 are associated with the default routing table (because they are not associated with a VRF). Therefore, the `clear ipv6 neighbor` command will clear ND cache entries on interfaces Ethernet 1/0 and Ethernet 2/0 only. In order to clear ND cache entries on interface Ethernet 0/0, the user must issue the `clear ipv6 neighbor vrf` red command.

```plaintext
interface ethernet0/0
  vrf forward red
  ipv6 address 2001:db8:1::1/64

interface ethernet1/0
  ipv6 address 2001:db8:2::1/64

interface ethernet2/0
  ipv6 address 2001:db8:3::1/64
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 neighbor</td>
<td>Configures a static entry in the IPv6 neighbor discovery cache.</td>
</tr>
<tr>
<td>show ipv6 neighbors</td>
<td>Displays IPv6 neighbor discovery cache information.</td>
</tr>
</tbody>
</table>
clear ipv6 nhrp

To clear all dynamic entries from the Next Hop Resolution Protocol (NHRP) cache, use the clear ipv6 nhrp command in privileged EXEC mode.

```
clear ipv6 nhrp [ipv6-address | counters]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>(Optional) The IPv6 network to delete.</td>
</tr>
<tr>
<td>counters</td>
<td>(Optional) Specifies NHRP counters to delete.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command does not clear any static (configured) IPv6-to-nonbroadcast multiaccess (NBMA) address mappings from the NHRP cache.

**Examples**

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

```
Device# clear ipv6 nhrp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 nhrp</td>
<td>Displays the NHRP cache.</td>
</tr>
</tbody>
</table>
clear ipv6 ospf

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the `clear ipv6 ospf` command in privileged EXEC mode.

```
clear ipv6 ospf [process-id] {process | force-spf | redistribution}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.</td>
</tr>
<tr>
<td>process</td>
<td>Restarts the OSPF process.</td>
</tr>
<tr>
<td>force-spf</td>
<td>Starts the shortest path first (SPF) algorithm without first clearing the OSPF database.</td>
</tr>
<tr>
<td>redistribution</td>
<td>Clears OSPF route redistribution.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `process` keyword is used with the `clear ipv6 ospf` command, the OSPF database is cleared and repopulated, and then the shortest path first (SPF) algorithm is performed. When the `force-spf` keyword is used with the `clear ipv6 ospf` command, the OSPF database is not cleared before the SPF algorithm is performed.

Use the `process-id` option to clear only one OSPF process. If the `process-id` option is not specified, all OSPF processes are cleared.

**Examples**

The following example starts the SPF algorithm without clearing the OSPF database:

```
Device# clear ipv6 ospf force-spf
```
clear ipv6 ospf counters

To clear the Open Shortest Path First (OSPF) state based on the OSPF routing process ID, use the `clear ipv6 ospf` command in privileged EXEC mode.

```
clear ipv6 ospf [process-id] counters [neighbor [neighbor-interfaceneighbor-id]]
```

**Syntax Description**

- **process-id** (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.
- **neighbor** (Optional) Neighbor statistics per interface or neighbor ID.
- **neighbor-interface** (Optional) Neighbor interface.
- **neighbor-id** (Optional) IPv6 or IP address of the neighbor.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `neighbor neighbor-interface` option to clear counters for all neighbors on a specified interface. If the `neighbor neighbor-interface` option is not used, all OSPF counters are cleared.

Use the `neighbor neighbor-id` option to clear counters at a specified neighbor. If the `neighbor neighbor-id` option is not used, all OSPF counters are cleared.

**Examples**

The following example provides detailed information on a neighbor router:

```
Device# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
   In the area 1 via interface Serial19/0
   Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
   Neighbor priority is 1, State is FULL, 6 state changes
   Options is 0x194AE05
   Dead timer due in 00:00:37
   Neighbor is up for 00:00:15
   Index 1/1/1, retransmission queue length 0, number of retransmission 1
   First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
   Last retransmission scan length is 1, maximum is 1
   Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following example clears all neighbors on the specified interface:

```
Device# clear ipv6 ospf counters neighbor s19/0
```

The following example now shows that there have been 0 state changes since the `clear ipv6 ospf counters neighbor s19/0` command was used:
Device# show ipv6 ospf neighbor detail
Neighbor 10.0.0.1
   In the area 1 via interface Serial19/0
   Neighbor:interface-id 21, link-local address FE80::A8BB:CCFF:FE00:6F00
   Neighbor priority is 1, State is FULL, 0 state changes
   Options is 0x194AE05
   Dead timer due in 00:00:39
   Neighbor is up for 00:00:43
   Index 1/1/1, retransmission queue length 0, number of retransmission 1
   First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
   Last retransmission scan length is 1, maximum is 1
   Last retransmission scan time is 0 msec, maximum is 0 msec

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf neighbor</td>
<td>Displays OSPF neighbor information on a per-interface basis.</td>
</tr>
</tbody>
</table>
clear ipv6 ospf events

To clear the Open Shortest Path First (OSPF) for IPv6 event log content based on the OSPF routing process ID, use the `clear ipv6 ospf events` command in privileged EXEC mode.

`clear ipv6 ospf [process-id] events`

**Syntax Description**

|process-id| (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the optional `process-id` argument to clear the IPv6 event log content of a specified OSPF routing process. If the `process-id` argument is not used, all event log content is cleared.

**Examples**

The following example enables the clearing of OSPF for IPv6 event log content for routing process 1:

```
Device# clear ipv6 ospf 1 events
```
clear ipv6 pim reset

To delete all entries from the topology table and reset the Multicast Routing Information Base (MRIB) connection, use the `clear ipv6 pim reset` command in privileged EXEC mode.

`clear ipv6 pim [vrf vrf-name] reset`

**Syntax Description**

| vrf vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using the `clear ipv6 pim reset` command breaks the PIM-MRIB connection, clears the topology table, and then reestablishes the PIM-MRIB connection. This procedure forces MRIB resynchronization.

**Caution**

Use the `clear ipv6 pim reset` command with caution, as it clears all PIM protocol information from the PIM topology table. Use of the `clear ipv6 pim reset` command should be reserved for situations where PIM and MRIB communication are malfunctioning.

**Examples**

The following example deletes all entries from the topology table and resets the MRIB connection:

```
Device# clear ipv6 pim reset
```
clear ipv6 pim topology

To clear the Protocol Independent Multicast (PIM) topology table, use the `clear ipv6 pim topology` command in privileged EXEC mode.

```
clear ipv6 pim [vrf vrf-name] topology [{group-name}group-address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>group-name</td>
<td>group-address</td>
</tr>
</tbody>
</table>

**Command Default**

When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command clears PIM protocol information from all group entries located in the PIM topology table. Information obtained from the MRIB table is retained. If a multicast group is specified, only those group entries are cleared.

**Examples**

The following example clears all group entries located in the PIM topology table:

```
Device# clear ipv6 pim topology
```
clear ipv6 pim traffic

To clear the Protocol Independent Multicast (PIM) traffic counters, use the clear ipv6 pim traffic command in privileged EXEC mode.

clear ipv6 pim [vrf vrf-name] traffic

Syntax Description

| Syntax Description | vrf vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

Command Default

When the command is used with no arguments, all traffic counters are cleared.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command clears PIM traffic counters. If the vrf vrf-name keyword and argument are used, only those counters are cleared.

Examples

The following example clears all PIM traffic counter:

Device# clear ipv6 pim traffic
clear ipv6 prefix-list

To reset the hit count of the IPv6 prefix list entries, use the clear ipv6 prefix-list command in privileged EXEC mode.

clear ipv6 prefix-list [prefix-list-name] [ipv6-prefix/prefix-length]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix-list-name</td>
<td>(Optional) The name of the prefix list from which the hit count is to be cleared.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>(Optional) The IPv6 network from which the hit count is to be cleared. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>/ prefix-length</td>
<td>(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
</tbody>
</table>

Command Default

The hit count is automatically cleared for all IPv6 prefix lists.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The clear ipv6 prefix-list command is similar to the clear ip prefix-list command, except that it is IPv6-specific.

The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

The following example clears the hit count from the prefix list entries for the prefix list named first_list that match the network mask 2001:0DB8::/35.

Device# clear ipv6 prefix-list first_list 2001:0DB8::/35

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 prefix-list</td>
<td>Creates an entry in an IPv6 prefix list.</td>
</tr>
<tr>
<td>ipv6 prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in an IPv6 prefix list.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Displays information about an IPv6 prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
clear ipv6 rip

To delete routes from the IPv6 Routing Information Protocol (RIP) routing table, use the `clear ipv6 rip` command in privileged EXEC mode.

```
clear ipv6 rip [name][vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>(Optional) Name of an IPv6 RIP process.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Clears information about the specified Virtual Routing and Forwarding (VRF) instance.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `name` argument is specified, only routes for the specified IPv6 RIP process are deleted from the IPv6 RIP routing table. If no `name` argument is specified, all IPv6 RIP routes are deleted.

Use the `show ipv6 rip` command to display IPv6 RIP routes.

Use the `clear ipv6 rip name vrf vrf-name` command to delete the specified VRF instances for the specified IPv6 RIP process.

**Examples**

The following example deletes all the IPv6 routes for the RIP process called one:

```
Device# clear ipv6 rip one
```

The following example deletes the IPv6 VRF instance, called vrf1 for the RIP process, called one:

```
Device# clear ipv6 rip one vrf vrf1
```

*Mar 15 12:36:17.022: [Exec]IPv6RIP[vrf1]: rip <name>, Delete all next-hops for 2001:DB8::1
*Mar 15 12:36:17.022: [Exec]IPv6RIP[vrf1]: rip <name>, Delete 2001:DB8::1 from table
*Mar 15 12:36:17.022: [IPv6 RIB Event Handler]IPv6RIP[<red>]: Event: 2001:DB8::1, Del, owner rip, previous None

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 rip</td>
<td>Displays the current contents of the IPv6 RIP routing table.</td>
</tr>
<tr>
<td>ipv6 rip vrf-mode enable</td>
<td>Enables VRF-aware support for IPv6 RIP.</td>
</tr>
<tr>
<td>show ipv6 rip</td>
<td>Displays the current content of the IPv6 RIP routing table.</td>
</tr>
</tbody>
</table>
clear ipv6 route

To delete routes from the IPv6 routing table, use the clear ipv6 route command in privileged EXEC mode.

```
clear ipv6 route {ipv6-address|ipv6-prefix/prefix-length} | *
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>The address of the IPv6 network to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>The IPv6 network number to delete from the table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>/ prefix-length</td>
<td>The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td>*</td>
<td>Clears all IPv6 routes.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The clear ipv6 route command is similar to the clear ip route command, except that it is IPv6-specific.

When the ipv6-address or ipv6-prefix/prefix-length argument is specified, only that route is deleted from the IPv6 routing table. When the * keyword is specified, all routes are deleted from the routing table (the per-destination maximum transmission unit [MTU] cache is also cleared).

### Examples

The following example deletes the IPv6 network 2001:0DB8::/35:

```
Device# clear ipv6 route 2001:0DB8::/35
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 route</td>
<td>Establishes static IPv6 routes.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays the current contents of the IPv6 routing table.</td>
</tr>
</tbody>
</table>
clear ipv6 spd

To clear the most recent Selective Packet Discard ( SPD) state transition, use the clear ipv6 spd command in privileged EXEC mode.

clear ipv6 spd

Syntax Description
This command has no arguments or keywords.

Command Modes
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The clear ipv6 spd command removes the most recent SPD state transition and any trend historical data.

Examples
The following example shows how to clear the most recent SPD state transition:

Device# clear ipv6 spd
**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.

```
default 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 default 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>attribute</code></td>
<td>(Optional) Enables NHRP attribute debugging operations.</td>
</tr>
<tr>
<td><code>cache</code></td>
<td>(Optional) Enables NHRP cache debugging operations.</td>
</tr>
<tr>
<td><code>condition</code></td>
<td>(Optional) Enables NHRP conditional debugging operations.</td>
</tr>
<tr>
<td><code>interface tunnel number</code></td>
<td>(Optional) Enables debugging operations for the tunnel interface.</td>
</tr>
<tr>
<td><code>nbma</code></td>
<td>(Optional) Enables debugging operations for the non-broadcast multiple access (NBMA) network.</td>
</tr>
<tr>
<td><code>ipv4-nbma-address</code></td>
<td>(Optional) Enables debugging operations based on the IPv4 address of the NBMA network.</td>
</tr>
<tr>
<td><code>nbma-name</code></td>
<td>(Optional) NBMA network name.</td>
</tr>
<tr>
<td><code>IPv6-address</code></td>
<td>(Optional) Enables debugging operations based on the IPv6 address of the NBMA network.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Enables debugging operations for the virtual routing and forwarding instance.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed logs of NHRP debugs.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>(Optional) Enables NHRP error debugging operations.</td>
</tr>
<tr>
<td><code>extension</code></td>
<td>(Optional) Enables NHRP extension processing debugging operations.</td>
</tr>
<tr>
<td><code>group</code></td>
<td>(Optional) Enables NHRP group debugging operations.</td>
</tr>
<tr>
<td><code>packet</code></td>
<td>(Optional) Enables NHRP activity debugging.</td>
</tr>
<tr>
<td><code>rate</code></td>
<td>(Optional) Enables NHRP rate limiting.</td>
</tr>
<tr>
<td><code>routing</code></td>
<td>(Optional) Enables NHRP routing debugging operations.</td>
</tr>
</tbody>
</table>

**Command Default**

NHRP debugging is not enabled.

**Command Modes**

Privileged EXEC (#)
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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: Send Registration Request via Tunnel0 vrf 0, packet size: 105
Aug 9 13:13:41.486: NHRP: netid_in = 0, to_us = 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip nhrp</td>
<td>Displays NHRP mapping information.</td>
</tr>
</tbody>
</table>
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.

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

**Syntax Description**

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

**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:

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show fhrp</td>
<td>Displays First Hop Redundancy Protocol (FHRP) information.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>track (VRRP)</td>
<td>Enables an object to be tracked using a VRRPv3 group.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>client-id</td>
<td>(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The <code>client-id interface-type number</code> option sets the client identifier to the hexadecimal MAC address of the named interface.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>hostname</td>
<td>(Optional) Specifies the hostname.</td>
</tr>
<tr>
<td>hostname</td>
<td>(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.</td>
</tr>
</tbody>
</table>

### 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)

### Usage Guidelines

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 aal5snap 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.

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` command.
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 17: Configuration Method and Resulting Contents of the DISCOVER Message**

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

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip dhcp pool</td>
<td>Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.</td>
</tr>
</tbody>
</table>
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**

- `name` Name of the DHCP pool. The IP address of the interface will be automatically configured from the DHCP pool specified in `name`.

**Command Default**

IP address pooling is disabled.

**Command Modes**

Interface configuration

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
</tbody>
</table>
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]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>Mask for the associated IP subnet.</td>
</tr>
<tr>
<td><code>secondary</code></td>
<td>(Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Name of the VRF table. The <code>vrf-name</code> argument specifies the VRF name of the ingress interface.</td>
</tr>
</tbody>
</table>

**Command Default**
No IP address is defined for the interface.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Command was introduced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 is the secondary address 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>match ip route-source</code></td>
<td>Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.</td>
</tr>
<tr>
<td><code>route-map</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or to enable policy routing.</td>
</tr>
<tr>
<td><code>set vrf</code></td>
<td>Enables VPN VRF selection within a route map for policy-based routing VRF selection.</td>
</tr>
<tr>
<td><code>show ip arp</code></td>
<td>Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.</td>
</tr>
<tr>
<td><code>show ip interface</code></td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show route-map</td>
<td>Displays static and dynamic route maps.</td>
</tr>
</tbody>
</table>
**ip nhrp authentication**

To configure the authentication string for an interface using the Next Hop Resolution Protocol (NHRP), use the `ip nhrp authentication` command in interface configuration mode. To remove the authentication string, use the `no` form of this command.

```
ip nhrp authentication string
no ip nhrp authentication [string]
```

**Syntax Description**

| string | Authentication string configured for the source and destination stations that controls whether NHRP stations allow intercommunication. The string can be up to eight characters long. |

**Command Default**

No authentication string is configured; the Cisco IOS software adds no authentication option to NHRP packets it generates.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All devices configured with NHRP within one logical nonbroadcast multiaccess (NBMA) network must share the same authentication string.

**Examples**

In the following example, the authentication string named specialxx must be configured in all devices using NHRP on the interface before NHRP communication occurs:

```
Device(config-if)# ip nhrp authentication specialxx
```
ip nhrp holdtime

To change the number of seconds that Next Hop Resolution Protocol (NHRP) nonbroadcast multiaccess (NBMA) addresses are advertised as valid in authoritative NHRP responses, use the `ip nhrp holdtime` command in interface configuration mode. To restore the default value, use the `no` form of this command.

```
ip nhrp holdtime seconds
no ip nhrp holdtime [seconds]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>seconds</th>
<th>Time in seconds that NBMA addresses are advertised as valid in positive authoritative NHRP responses.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>The recommended NHRP hold time value ranges from 300 to 600 seconds. Although a higher value can be used when required, we recommend that you do not use a value less than 300 seconds; and if used, it should be used with extreme caution.</td>
</tr>
</tbody>
</table>

**Command Default**

7200 seconds (2 hours)

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip nhrp holdtime` command affects authoritative responses only. The advertised holding time is the length of time the Cisco IOS software tells other routers to keep information that it is providing in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the holding time expires.

The NHRP cache can contain static and dynamic entries. The static entries never expire. Dynamic entries expire regardless of whether they are authoritative or nonauthoritative.

**Examples**

In the following example, NHRP NBMA addresses are advertised as valid in positive authoritative NHRP responses for 1 hour:

```
Device(config-if)# ip nhrp holdtime 3600
```
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 interface configuration command. To remove the static entry from Next Hop Resolution Protocol (NHRP) cache, use the no form of this command.

```
ip nhrp map {ip-address [nbma-ip-address][dest-mask][nbma-ipv6-address] | multicast
{nbma-ip-address nbma-ipv6-address | dynamic}}
no ip nhrp map {ip-address [nbma-ip-address][dest-mask][nbma-ipv6-address] | multicast
{nbma-ip-address nbma-ipv6-address | dynamic}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the destinations reachable through the Nonbroadcast multiaccess (NBMA) network. This address is mapped to the NBMA address.</td>
</tr>
<tr>
<td>nbma-ip-address</td>
<td>NBMA IP address.</td>
</tr>
<tr>
<td>dest-mask</td>
<td>Destination network address for which a mask is required.</td>
</tr>
<tr>
<td>nbma-ipv6-address</td>
<td>NBMA IPv6 address.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Dynamically learns destinations from client registrations on hub.</td>
</tr>
<tr>
<td>multicast</td>
<td>NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium you are using. 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.</td>
</tr>
</tbody>
</table>

### Command Default

No static IP-to-NBMA cache entries exist.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You will probably need to configure at least one static mapping in order to reach the next-hop server. Repeat this command to statically configure multiple IP-to-NBMA address mappings.

### 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 to be 192.0.0.1 and the NBMA address for 10.0.1.3 is 192.2.7.8.

```
Device(config)# interface tunnel 0
Device(config-if)# ip nhrp nhs 10.0.0.1
Device(config-if)# ip nhrp nhs 10.0.1.3
Device(config-if)# ip nhrp map 10.0.0.1 192.0.0.1
Device(config-if)# ip nhrp map 10.0.1.3 192.2.7.8
```
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. Addresses 10.0.0.1 and 10.0.0.2 are the IP addresses of two other routers that are part of the tunnel network, but those addresses are their addresses in the underlying network, not the tunnel network. They would have tunnel addresses that are in network 10.0.0.0.

```
Device(config)# interface tunnel 0
Device(config-if)# ip address 10.0.0.3 255.0.0.0
Device(config-if)# ip nhrp map multicast 10.0.0.1
Device(config-if)# ip nhrp map multicast 10.0.0.2
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip nhrp</td>
<td>Clears all dynamic entries from the NHRP cache.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-nbma-address</code></td>
<td>NBMA address that is directly reachable through the NBMA network. The address format varies depending on the medium that you are using.</td>
</tr>
<tr>
<td><code>ipv6-nbma-address</code></td>
<td>IPv6 NBMA address.</td>
</tr>
<tr>
<td><code>dynamic</code></td>
<td>Dynamically learns destinations from client registrations on the hub.</td>
</tr>
</tbody>
</table>

**Command Default**

No NBMA addresses are configured as destinations for broadcast or multicast packets.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Denali 16.5.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug nhrp</td>
<td>Enables NHRP debugging.</td>
</tr>
<tr>
<td>interface</td>
<td>Configures an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>tunnel destination</td>
<td>Specifies the destination for a tunnel interface.</td>
</tr>
</tbody>
</table>
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**
- **number**: 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 the interface.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config-if)# ip nhrp network-id 1
```
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-addressFQDN-string] [multicast] [priority value] [cluster value] | cluster value max-connections value | dynamic nbma nbma-addressFQDN-string [multicast] [priority value] | cluster value | fallback seconds} 
no ip nhrp nhs {nhs-address nbma-addressFQDN-string} [multicast] [priority value] | cluster value | cluster value max-connections value | dynamic nbma nbma-addressFQDN-string | multicast] [priority value] | cluster value | fallback seconds}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nhs-address</td>
<td>Address of the next-hop server being specified.</td>
</tr>
<tr>
<td>net-address</td>
<td>(Optional) IP address of a network served by the next-hop server.</td>
</tr>
<tr>
<td>netmask</td>
<td>(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.</td>
</tr>
<tr>
<td>nbma</td>
<td>(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.</td>
</tr>
<tr>
<td>nbma-address</td>
<td>NBMA address.</td>
</tr>
<tr>
<td>FQDN-string</td>
<td>Next hop server (NHS) fully qualified domain name (FQDN) string.</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.</td>
</tr>
<tr>
<td>priority value</td>
<td>(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.</td>
</tr>
<tr>
<td>cluster value</td>
<td>(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.</td>
</tr>
<tr>
<td>max-connections value</td>
<td>Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Configures the spoke to learn the NHS protocol address dynamically.</td>
</tr>
<tr>
<td>fallback seconds</td>
<td>Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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.

When the `ip nhrp nhs dynamic` command is configured on a DMVPN tunnel and the `shut` command is issued to the tunnel interface, the crypto socket does not receive shut message, thereby not bringing up a DMVPN session with the hub.

For any next hop server that is configured, you can specify multiple networks by repeating this 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:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(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:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Device# configure terminal
Device(config)# interface tunnel 1
Device(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nhrp map</code></td>
<td>Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.</td>
</tr>
<tr>
<td><code>show ip nhrp</code></td>
<td>Displays NHRP mapping information.</td>
</tr>
</tbody>
</table>
ip nhrp registration

To set the time between periodic registration messages in the Next Hop Resolution Protocol (NHRP) request and reply packets, use the `ip nhrp registration` command in interface configuration mode. To disable this functionality, use the `no` form of this command.

```
ip nhrp registration timeout seconds
no ip nhrp registration timeout seconds
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Time between periodic registration messages.</td>
</tr>
<tr>
<td></td>
<td>• <code>seconds</code>—Number of seconds. The range is from 1 through the value of the</td>
</tr>
<tr>
<td></td>
<td>NHRP hold timer.</td>
</tr>
<tr>
<td></td>
<td>• If the <code>timeout</code> keyword is not specified, NHRP registration messages are</td>
</tr>
<tr>
<td></td>
<td>sent every number of seconds equal to 1/3 the value of the NHRP hold timer.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is not enabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.8.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to set the time between periodic registration in the Next Hop Resolution Protocol (NHRP) request and reply packets.

**Examples**

The following example shows that the registration timeout is set to 120 seconds:

```
Device(config)# interface tunnel 4
Device(config-if)# ip nhrp registration timeout 120
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nhrp holdtime</code></td>
<td>Changes the number of seconds that NHRP NBMA addresses are advertised as valid in authoritative NHRP responses</td>
</tr>
</tbody>
</table>
**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
no ipv6 access-list access-list-name
```

**Syntax Description**

| Access-list-name | Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric. |

**Command Default**

No IPv6 access list is defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 access-list` command is similar to the `ip access-list` command, except that it is IPv6-specific.

The standard IPv6 ACL functionality supports—in addition to traffic filtering based on source and destination addresses—filtering of traffic based on IPv6 option headers and optional, upper-layer protocol type information for finer granularity of control (functionality similar to extended ACLs in IPv4). 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.

For backward compatibility, the `ipv6 access-list` command with the `deny` and `permit` keywords in global configuration mode is still supported; however, an IPv6 ACL defined with deny and permit conditions in global configuration mode is translated to IPv6 access list configuration mode.

Refer to the deny (IPv6) and permit (IPv6) commands for more information on filtering IPv6 traffic based on IPv6 option headers and optional, upper-layer protocol type information. See the "Examples" section for an example of a translated IPv6 ACL configuration.
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.

Note
IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

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.

Note
An IPv6 ACL applied to an interface with the ipv6 traffic-filter command filters traffic that is forwarded, not originated, by the device.

Note
When using this command to modify an ACL that is already associated with a bootstrap router (BSR) candidate rendezvous point (RP) (see the ipv6 pim bsr candidate rp command) or a static RP (see the ipv6 pim rp-address command), any added address ranges that overlap the PIM SSM group address range (FF3x::/96) are ignored. A warning message is generated and the overlapping address ranges are added to the ACL, but they have no effect on the operation of the configured BSR candidate RP or static RP commands.

Duplicate remark statements can no longer be configured from the IPv6 access control list. Because each remark statement is a separate entity, each one is required to be unique.

Examples
The following example is from a device running Cisco IOS Release 12.0(23)S or later releases. 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 is from a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S. The 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

If the same configuration was entered on a device running Cisco IOS Release 12.0(23)S or later releases, the configuration would be translated into IPv6 access list configuration mode as follows:

ipv6 access-list list2
deny FEC0:0:0:2::/64 any
permit ipv6 any any
interface ethernet 0
ipv6 traffic-filter list2 out

**Note** 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.

**Note** IPv6 ACLs defined on a device running Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, or 12.0(22)S that rely on the implicit deny condition or specify a **deny any any** statement to filter traffic should contain **permit** statements for link-local and multicast addresses to avoid the filtering of protocol packets (for example, packets associated with the neighbor discovery protocol). Additionally, IPv6 ACLs that use **deny** statements to filter traffic should use a **permit any any** statement as the last statement in the list.

**Note** An IPv6 device will not forward to another network an IPv6 packet that has a link-local address as either its source or destination address (and the source interface for the packet is different from the destination interface for the packet).

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny (IPv6)</td>
<td>Sets deny conditions for an IPv6 access list.</td>
</tr>
<tr>
<td>ipv6 access-class</td>
<td>Filters incoming and outgoing connections to and from the device based on an IPv6 access list.</td>
</tr>
<tr>
<td>ipv6 pim bsr candidate rp</td>
<td>Configures the candidate RP to send PIM RP advertisements to the BSR.</td>
</tr>
<tr>
<td>ipv6 pim rp-address</td>
<td>Configure the address of a PIM RP for a particular group range.</td>
</tr>
<tr>
<td>ipv6 traffic-filter</td>
<td>Filters incoming or outgoing IPv6 traffic on an interface.</td>
</tr>
<tr>
<td>permit (IPv6)</td>
<td>Sets permit conditions for an IPv6 access list.</td>
</tr>
<tr>
<td>show ipv6 access-list</td>
<td>Displays the contents of all current IPv6 access lists.</td>
</tr>
</tbody>
</table>
ipv6 address-validate

To enable IPv6 address validation, use the **ipv6 address-validate** in global configuration mode. To disable IPv6 address validation, use the **no** form of this command.

**ipv6 address-validate**

**no ipv6 address-validate**

**Command Default**

This command is enabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ipv6 address-validate** command is used to validate whether the interface identifiers in an assigned IPv6 address are a part of the reserved IPv6 interface identifiers range, as specified in RFC5453. If the interface identifiers of the assigned IPv6 address are a part of the reserved range, a new IPv6 address is assigned.

Only auto-configured addresses or addresses configured by DHCPv6 are validated.

**Note**

The **no ipv6-address validate** command disables the IPv6 address validation and allows assigning of IPv6 addresses with interface identifiers that are a part of the reserved IPv6 interface identifiers range. We do not recommend the use of this command.

**Examples**

The following example shows how to re-enable IPv6 address validation if it is disabled using the no ipv6-address validate command:

```
Device> enable
Device# configure terminal
Device{config}# ipv6 address-validate
```
ipv6 cef

To enable Cisco Express Forwarding for IPv6, use the `ipv6 cef` command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the `no` form of this command.

```
ipv6 cef
no ipv6 cef
```

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

**Command Default**
Cisco Express Forwarding for IPv6 is disabled by default.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `ipv6 cef` command is similar to the `ip cef` command, except that it is IPv6-specific.
The `ipv6 cef` command is not available on the Cisco 12000 series Internet routers because this distributed platform operates only in distributed Cisco Express Forwarding for IPv6 mode.

**Note**
The `ipv6 cef` command is not supported in interface configuration mode.

**Note**
Some distributed architecture platforms support both Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6. When Cisco Express Forwarding for IPv6 is configured on distributed platforms, Cisco Express Forwarding switching is performed by the Route Processor (RP).

**Note**
You must enable Cisco Express Forwarding for IPv4 by using the `ip cef` global configuration command before enabling Cisco Express Forwarding for IPv6 by using the `ipv6 cef` global configuration command.

Cisco Express Forwarding for IPv6 is advanced Layer 3 IP switching technology that functions the same and offer the same benefits as Cisco Express Forwarding for IPv4. Cisco Express Forwarding for IPv6 optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

**Examples**
The following example enables standard Cisco Express Forwarding for IPv4 operation and then standard Cisco Express Forwarding for IPv6 operation globally on the Device.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route-cache</td>
<td>Controls the use of high-speed switching caches for IP routing.</td>
</tr>
<tr>
<td>show cef</td>
<td>Displays which packets the line cards dropped or displays which packets were not express-forwarded.</td>
</tr>
<tr>
<td>show ipv6 cef</td>
<td>Displays entries in the IPv6 FIB.</td>
</tr>
</tbody>
</table>
**ipv6 cef accounting**

To enable Cisco Express Forwarding for IPv6 and distributed Cisco Express Forwarding for IPv6 network accounting, use the `ipv6 cef accounting` command in global configuration mode or interface configuration mode. To disable Cisco Express Forwarding for IPv6 network accounting, use the `no` form of this command.

```
ipv6 cef accounting accounting-types
no ipv6 cef accounting accounting-types
```

### Specific Cisco Express Forwarding Accounting Information Through Interface Configuration Mode

```
ipv6 cef accounting non-recursive {external | internal}
no ipv6 cef accounting non-recursive {external | internal}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>accounting-types</th>
<th>The <code>accounting-types</code> argument must be replaced with at least one of the following keywords. Optionally, you can follow this keyword by any or all of the other keywords, but you can use each keyword only once.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>load-balance-hash</td>
<td>--Enables load balancing hash bucket counters.</td>
</tr>
<tr>
<td></td>
<td>non-recursive</td>
<td>--Enables accounting through nonrecursive prefixes.</td>
</tr>
<tr>
<td></td>
<td>per-prefix</td>
<td>--Enables express forwarding of the collection of the number of packets and bytes to a destination (or prefix).</td>
</tr>
<tr>
<td></td>
<td>prefix-length</td>
<td>--Enables accounting through prefix length.</td>
</tr>
</tbody>
</table>

| non-recursive       | Enables accounting through nonrecursive prefixes. |
|                     | This keyword is optional when used in global configuration mode after another keyword is entered. See the `accounting-types` argument. |

| external            | Counts input traffic in the nonrecursive external bin. |
| internal             | Counts input traffic in the nonrecursive internal bin. |

**Command Default**

Cisco Express Forwarding for IPv6 network accounting is disabled by default.

**Command Modes**

Global configuration (config)

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 cef accounting` command is similar to the `ip cef accounting` command, except that it is IPv6-specific. Configuring Cisco Express Forwarding for IPv6 network accounting enables you to collect statistics on Cisco Express Forwarding for IPv6 traffic patterns in your network.
When you enable network accounting for Cisco Express Forwarding for IPv6 by using the `ipv6 cef accounting` command in global configuration mode, accounting information is collected at the Route Processor (RP) when Cisco Express Forwarding for IPv6 mode is enabled and at the line cards when distributed Cisco Express Forwarding for IPv6 mode is enabled. You can then display the collected accounting information using the `show ipv6 cef` EXEC command.

For prefixes with directly connected next hops, the `non-recursive` keyword enables express forwarding of the collection of packets and bytes through a prefix. This keyword is optional when this command is used in global configuration mode after you enter another keyword on the `ipv6 cef accounting` command.

This command in interface configuration mode must be used in conjunction with the global configuration command. The interface configuration command allows a user to specify two different bins (internal or external) for the accumulation of statistics. The internal bin is used by default. The statistics are displayed through the `show ipv6 cef detail` command.

Per-destination load balancing uses a series of 16 hash buckets into which the set of available paths are distributed. A hash function operating on certain properties of the packet is applied to select a bucket that contains a path to use. The source and destination IP addresses are the properties used to select the bucket for per-destination load balancing. Use the `load-balance-hash` keyword with the `ipv6 cef accounting` command to enable per-hash-bucket counters. Enter the `show ipv6 cef prefix internal` command to display the per-hash-bucket counters.

### Examples

The following example enables the collection of Cisco Express Forwarding for IPv6 accounting information for prefixes with directly connected next hops:

```
Device(config)# ipv6 cef accounting non-recursive
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip cef accounting</code></td>
<td>Enable Cisco Express Forwarding network accounting (for IPv4).</td>
</tr>
<tr>
<td><code>show cef</code></td>
<td>Displays information about packets forwarded by Cisco Express Forwarding.</td>
</tr>
<tr>
<td><code>show ipv6 cef</code></td>
<td>Displays entries in the IPv6 FIB.</td>
</tr>
</tbody>
</table>
ipv6 cef distributed

To enable distributed Cisco Express Forwarding for IPv6, use the `ipv6 cef distributed` command in global configuration mode. To disable Cisco Express Forwarding for IPv6, use the `no` form of this command.

```
ipv6 cef distributed
no ipv6 cef distributed
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Distributed Cisco Express Forwarding for IPv6 is disabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 cef distributed` command is similar to the `ip cef distributed` command, except that it is IPv6-specific. Enabling distributed Cisco Express Forwarding for IPv6 globally on the router by using the `ipv6 cef distributed` in global configuration mode distributes the Cisco Express Forwarding processing of IPv6 packets from the Route Processor (RP) to the line cards of distributed architecture platforms.

**Note**

To forward distributed Cisco Express Forwarding for IPv6 traffic on the router, configure the forwarding of IPv6 unicast datagrams globally on your router by using the `ipv6 unicast-routing` global configuration command, and configure an IPv6 address and IPv6 processing on an interface by using the `ipv6 address` interface configuration command.

**Note**

You must enable distributed Cisco Express Forwarding for IPv4 by using the `ip cef distributed` global configuration command before enabling distributed Cisco Express Forwarding for IPv6 by using the `ipv6 cef distributed` global configuration command.

Cisco Express Forwarding is advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with web-based applications and interactive sessions.

**Examples**

The following example enables distributed Cisco Express Forwarding for IPv6 operation:

```
Device(config)# ipv6 cef distributed
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip route-cache</td>
<td>Controls the use of high-speed switching caches for IP routing.</td>
</tr>
<tr>
<td>show ipv6 cef</td>
<td>Displays entries in the IPv6 FIB.</td>
</tr>
</tbody>
</table>
ipv6 cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm for IPv6, use the `ipv6 cef load-sharing algorithm` command in global configuration mode. To return to the default universal load-balancing algorithm, use the `no` form of this command.

```
ipv6 cef load-sharing algorithm {original | universal [id]}
no ipv6 cef load-sharing algorithm
```

| Syntax Description | original | Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.
| universal          | Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.
| id                | (Optional) Fixed identifier in hexadecimal format.

**Command Default**

The universal load-balancing algorithm is selected by default. If you do not configure the fixed identifier for a load-balancing algorithm, the device automatically generates a unique ID.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 cef load-sharing algorithm` command is similar to the `ip cef load-sharing algorithm` command, except that it is IPv6-specific.

When the Cisco Express Forwarding for IPv6 load-balancing algorithm is set to universal mode, each device on the network can make a different load-sharing decision for each source-destination address pair.

**Examples**

The following example shows how to enable the Cisco Express Forwarding original load-balancing algorithm for IPv6:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 cef load-sharing algorithm original
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip cef load-sharing algorithm</code></td>
<td>Selects a Cisco Express Forwarding load-balancing algorithm (for IPv4).</td>
</tr>
</tbody>
</table>
ipv6 cef optimize neighbor resolution

To configure address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the `ipv6 cef optimize neighbor resolution` command in global configuration mode. To disable address resolution optimization from Cisco Express Forwarding for IPv6 for directly connected neighbors, use the `no` form of this command.

```
ipv6 cef optimize neighbor resolution
no ipv6 cef optimize neighbor resolution
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

If this command is not configured, Cisco Express Forwarding for IPv6 does not optimize the address resolution of directly connected neighbors.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 cef optimize neighbor resolution` command is very similar to the `ip cef optimize neighbor resolution` command, except that it is IPv6-specific.

Use this command to trigger Layer 2 address resolution of neighbors directly from Cisco Express Forwarding for IPv6.

**Examples**

The following example shows how to optimize address resolution from Cisco Express Forwarding for IPv6 for directly connected neighbors:

```
Device(config)# ipv6 cef optimize neighbor resolution
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip cef optimize neighbor resolution</code></td>
<td>Configures address resolution optimization from Cisco Express Forwarding for IPv4 for directly connected neighbors.</td>
</tr>
</tbody>
</table>
ipv6 destination-guard policy

To define a destination guard policy, use the `ipv6 destination-guard policy` command in global configuration mode. To remove the destination guard policy, use the `no` form of this command.

```
ipv6 destination-guard policy [policy-name]
no ipv6 destination-guard policy [policy-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>policy-name</code></td>
<td>(Optional) Name of the destination guard policy.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>No destination guard policy is defined.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration (config)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>This command enters destination-guard configuration mode. The destination guard policies can be used to filter IPv6 traffic based on the destination address to block data traffic from an unknown source.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example shows how to define the name of a destination guard policy:</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```
Device(config)#ipv6 destination-guard policy policy1
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>Description</td>
<td>Syntax</td>
</tr>
<tr>
<td><code>show ipv6 destination-guard policy</code></td>
<td>Displays destination guard information.</td>
<td></td>
</tr>
</tbody>
</table>
ipv6 dhcp-relay bulk-lease

To configure bulk lease query parameters, use the `ipv6 dhcp-relay bulk-lease` command in global configuration mode. To remove the bulk-lease query configuration, use the `no` form of this command.

```
ipv6 dhcp-relay bulk-lease {data-timeout seconds | retry number} [disable]
no ipv6 dhcp-relay bulk-lease [disable]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>data-timeout</code></td>
<td>(Optional) Bulk lease query data transfer timeout.</td>
</tr>
<tr>
<td><code>seconds</code></td>
<td>(Optional) The range is from 60 seconds to 600 seconds. The default is 300 seconds.</td>
</tr>
<tr>
<td><code>retry</code></td>
<td>(Optional) Sets the bulk lease query retries.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>(Optional) The range is from 0 to 5. The default is 5.</td>
</tr>
<tr>
<td><code>disable</code></td>
<td>(Optional) Disables the DHCPv6 bulk lease query feature.</td>
</tr>
</tbody>
</table>

**Command Default**

Bulk lease query is enabled automatically when the DHCP for IPv6 (DHCPv6) relay agent feature is enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 dhcp-relay bulk-lease` command in global configuration mode to configure bulk lease query parameters, such as data transfer timeout and bulk-lease TCP connection retries.

The DHCPv6 bulk lease query feature is enabled automatically when the DHCPv6 relay agent is enabled. The DHCPv6 bulk lease query feature itself cannot be enabled using this command. To disable this feature, use the `ipv6 dhcp-relay bulk-lease` command with the `disable` keyword.

**Examples**

The following example shows how to set the bulk lease query data transfer timeout to 60 seconds:

```
Device(config)# ipv6 dhcp-relay bulk-lease data-timeout 60
```
ipv6 dhcp-relay option vpn

To enable the DHCP for IPv6 relay VRF-aware feature, use the `ipv6 dhcp-relay option vpn` command in global configuration mode. To disable the feature, use the `no` form of this command.

```
ipv6 dhcp-relay option vpn
no ipv6 dhcp-relay option vpn
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The DHCP for IPv6 relay VRF-aware feature is not enabled on the device.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 dhcp-relay option vpn` command allows the DHCPv6 relay VRF-aware feature to be enabled globally on the device. If the `ipv6 dhcp relay option vpn` command is enabled on a specified interface, it overrides the global `ipv6 dhcp-relay option vpn` command.

**Examples**

The following example enables the DHCPv6 relay VRF-aware feature globally on the device:

```
Device(config)# ipv6 dhcp-relay option vpn
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 dhcp relay option vpn</code></td>
<td>Enables the DHCPv6 relay VRF-aware feature on an interface.</td>
</tr>
</tbody>
</table>
ipv6 dhcp-relay source-interface

To configure an interface to use as the source when relaying messages, use the `ipv6 dhcp-relay source-interface` command in global configuration mode. To remove the interface from use as the source, use the `no` form of this command.

`ipv6 dhcp-relay source-interface interface-type interface-number`
`no ipv6 dhcp-relay source-interface interface-type interface-number`

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Interface type and number that specifies output interface for a destination. If this argument is configured, client messages are forwarded to the destination address through the link to which the output interface is connected.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

The address of the server-facing interface is used as the IPv6 relay source.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the configured interface is shut down, or if all of its IPv6 addresses are removed, the relay will revert to its standard behavior.

The interface configuration (using the `ipv6 dhcp relay source-interface` command in interface configuration mode) takes precedence over the global configuration if both have been configured.

**Examples**

The following example configures the Loopback 0 interface to be used as the relay source:

```
Device(config)# ipv6 dhcp-relay source-interface loopback 0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 dhcp relay source-interface</code></td>
<td>Enables DHCP for IPv6 service on an interface.</td>
</tr>
</tbody>
</table>
ipv6 dhcp binding track ppp

To configure Dynamic Host Configuration Protocol (DHCP) for IPv6 to release any bindings associated with a PPP connection when that connection closes, use the `ipv6 dhcp binding track ppp` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
ipv6 dhcp binding track ppp
no ipv6 dhcp binding track ppp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

When a PPP connection closes, the DHCP bindings associated with that connection are not released.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 dhcp binding track ppp` command configures DHCP for IPv6 to automatically release any bindings associated with a PPP connection when that connection is closed. The bindings are released automatically to accommodate subsequent new registrations by providing sufficient resource.

**Note**

In IPv6 broadband deployment using DHCPv6, you must enable release of prefix bindings associated with a PPP virtual interface using this command. This ensures that DHCPv6 bindings are tracked together with PPP sessions, and in the event of DHCP REBIND failure, the client initiates DHCPv6 negotiation again.

A binding table entry on the DHCP for IPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding voluntarily, all prefixes’ valid lifetimes have expired, or an administrator clears the binding.

**Examples**

The following example shows how to release the prefix bindings associated with the PPP:

```plaintext
Device(config)# ipv6 dhcp binding track ppp
```
ipv6 dhcp database

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent, use the `ipv6 dhcp database` command in global configuration mode. To delete the database agent, use the `no` form of this command.

```
ipv6 dhcp database agent [write-delay seconds] [timeout seconds]
no ipv6 dhcp database agent
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>agent</code></td>
<td>A flash, local bootflash, compact flash, NVRAM, FTP, TFTP, or Remote Copy</td>
</tr>
<tr>
<td></td>
<td>Protocol (RCP) uniform resource locator.</td>
</tr>
<tr>
<td><code>write-delay seconds</code></td>
<td>(Optional) How often (in seconds) DHCP for IPv6 sends database updates. The</td>
</tr>
<tr>
<td></td>
<td>default is 300 seconds. The minimum write delay is 60 seconds.</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) How long, in seconds, the router waits for a database transfer.</td>
</tr>
</tbody>
</table>

**Command Default**

Write-delay default is 300 seconds. Timeout default is 300 seconds.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 dhcp database` command specifies DHCP for IPv6 binding database agent parameters. The user may configure multiple database agents.

A binding table entry is automatically created whenever a prefix is delegated to a client from the configuration pool, updated when the client renews, rebinds, or confirms the prefix delegation, and deleted when the client releases all the prefixes in the binding voluntarily, all prefixes’ valid lifetimes have expired, or administrators enable the clear `ipv6 dhcp binding` command. These bindings are maintained in RAM and can be saved to permanent storage using the `agent` argument so that the information about configuration such as prefixes assigned to clients is not lost after a system reload or power down. The bindings are stored as text records for easy maintenance.

Each permanent storage to which the binding database is saved is called the database agent. A database agent can be a remote host such as an FTP server or a local file system such as NVRAM.

The `write-delay` keyword specifies how often, in seconds, that DHCP sends database updates. By default, DHCP for IPv6 server waits 300 seconds before sending any database changes.

The `timeout` keyword specifies how long, in seconds, the router waits for a database transfer. Infinity is defined as 0 seconds, and transfers that exceed the timeout period are aborted. By default, the DHCP for IPv6 server waits 300 seconds before aborting a database transfer. When the system is going to reload, there is no transfer timeout so that the binding table can be stored completely.

**Examples**

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in TFTP:
Device(config)# ipv6 dhcp database tftp://10.0.0.1/dhcp-binding

The following example specifies DHCP for IPv6 binding database agent parameters and stores binding entries in bootflash:
Device(config)# ipv6 dhcp database bootflash

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp binding</td>
<td>Deletes automatic client bindings from the DHCP for IPv6 server binding table</td>
</tr>
<tr>
<td>show ipv6 dhcp database</td>
<td>Displays DHCP for IPv6 binding database agent information.</td>
</tr>
</tbody>
</table>
ipv6 dhcp iana-route-add

To add routes for individually assigned IPv6 addresses on a relay or server, use the `ipv6 dhcp iana-route-add` command in global configuration mode. To disable route addition for individually assigned IPv6 addresses on a relay or server, use the `no` form of the command.

```
ipv6 dhcp iana-route-add
no ipv6 dhcp iana-route-add
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Route addition for individually assigned IPv6 addresses on a relay or server is disabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 dhcp iana-route-add` command is disabled by default and has to be enabled if route addition is required. Route addition for Internet Assigned Numbers Authority (IANA) is possible if the client is connected to the relay or server through unnumbered interfaces, and if route addition is enabled with the help of this command.

**Examples**

The following example shows how to enable route addition for individually assigned IPv6 addresses:

```
Device(config)# ipv6 dhcp iana-route-add
```
**ipv6 dhcp iapd-route-add**

To enable route addition by Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay and server for the delegated prefix, use the `ipv6 dhcp iapd-route-add` command in global configuration mode. To disable route addition, use the `no` form of the command.

```
ipv6 dhcp iapd-route-add
no ipv6 dhcp iapd-route-add
```

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

**Command Default**
DHCPv6 relay and DHCPv6 server add routes for delegated prefixes by default.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The DHCPv6 relay and the DHCPv6 server add routes for delegated prefixes by default. The presence of this command on a device does not mean that routes will be added on that device. When you configure the command, routes for delegated prefixes will only be added on the first Layer 3 relay and server.

**Examples**
The following example shows how to enable the DHCPv6 relay and server to add routes for a delegated prefix:

```
Device(config)# ipv6 dhcp iapd-route-add
```
ipv6 dhcp-ldra

To enable Lightweight DHCPv6 Relay Agent (LDRA) functionality on an access node, use the `ipv6 dhcp-ldra` command in global configuration mode. To disable the LDRA functionality, use the `no` form of this command.

```
ipv6 dhcp-ldra {enable | disable}
no ipv6 dhcp-ldra {enable | disable}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables LDRA functionality on an access node.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables LDRA functionality on an access node.</td>
</tr>
</tbody>
</table>

**Command Default**

By default, LDRA functionality is not enabled on an access node.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the LDRA functionality globally using the `ipv6 dhcp-ldra` command before configuring it on a VLAN or an access node (such as a Digital Subscriber Link Access Multiplexer [DSLAM] or an Ethernet switch) interface.

**Example**

The following example shows how to enable the LDRA functionality:

```
Device(config)# ipv6 dhcp-ldra enable
Device(config)# exit
```

**Note**

In the above example, Device denotes an access node.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp ldra attach-policy</td>
<td>Enables LDRA functionality on a VLAN.</td>
</tr>
<tr>
<td>ipv6 dhcp-ldra attach-policy</td>
<td>Enables LDRA functionality on an interface.</td>
</tr>
</tbody>
</table>
**ipv6 dhcp ping packets**

To specify the number of packets a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server sends to a pool address as part of a ping operation, use the `ipv6 dhcp ping packets` command in global configuration mode. To prevent the server from pinging pool addresses, use the `no` form of this command.

```
ipv6 dhcp ping packets number
```

**Syntax Description**

| number | The number of ping packets sent before the address is assigned to a requesting client. The valid range is from 0 to 10. |

**Command Default**

No ping packets are sent before the address is assigned to a requesting client.

**Command Modes**

Global configuration (``#``)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The DHCPv6 server pings a pool address before assigning the address to a requesting client. If the ping is unanswered, the server assumes, with a high probability, that the address is not in use and assigns the address to the requesting client.

Setting the `number` argument to 0 turns off the DHCPv6 server ping operation.

**Examples**

The following example specifies four ping attempts by the DHCPv6 server before further ping attempts stop:

```
Device(config)# ipv6 dhcp ping packets 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>clear ipv6 dhcp conflict</code></td>
<td>Clears an address conflict from the DHCPv6 server database.</td>
</tr>
<tr>
<td><code>show ipv6 dhcp conflict</code></td>
<td>Displays address conflicts found by a DHCPv6 server, or reported through a DECLINE message from a client.</td>
</tr>
</tbody>
</table>
### ipv6 dhcp pool

To configure a Dynamic Host Configuration Protocol (DHCP) for IPv6 server configuration information pool and enter DHCP for IPv6 pool configuration mode, use the `ipv6 dhcp pool` command in global configuration mode. To delete a DHCP for IPv6 pool, use the `no` form of this command.

```
ipv6 dhcp pool poolname
no ipv6 dhcp pool poolname
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>poolname</th>
<th>User-defined name for the local prefix pool. The pool name can be a symbolic string (such as &quot;Engineering&quot;) or an integer (such as 0).</th>
</tr>
</thead>
</table>

**Command Default**

DHCP for IPv6 pools are not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 dhcp pool` command to create a DHCP for IPv6 server configuration information pool. When the `ipv6 dhcp pool` command is enabled, the configuration mode changes to DHCP for IPv6 pool configuration mode. In this mode, the administrator can configure pool parameters, such as prefixes to be delegated and Domain Name System (DNS) servers, using the following commands:

- **address prefix** `IPv6-prefix [lifetime {valid-lifetime preferred-lifetime infinite}]` sets an address prefix for address assignment. This address must be in hexadecimal, using 16-bit values between colons.
- **link-address** `IPv6-prefix` sets a link-address IPv6 prefix. When an address on the incoming interface or a link-address in the packet matches the specified IPv6-prefix, the server uses the configuration information pool. This address must be in hexadecimal, using 16-bit values between colons.
- **vendor-specific** `vendor-id` enables DHCPv6 vendor-specific configuration mode. Specify a vendor identification number. This number is the vendor IANA Private Enterprise Number. The range is 1 to 4294967295. The following configuration command is available:
  - **suboption number** sets vendor-specific suboption number. The range is 1 to 65535. You can enter an IPv6 address, ASCII text, or a hex string as defined by the suboption parameters.

**Note**

The `hex` value used under the `suboption` keyword allows users to enter only hex digits (0-f). Entering an invalid `hex` value does not delete the previous configuration.

Once the DHCP for IPv6 configuration information pool has been created, use the `ipv6 dhcp server` command to associate the pool with a server on an interface. If you do not configure an information pool, you need to use the `ipv6 dhcp server interface` configuration command to enable the DHCPv6 server function on an interface.
When you associate a DHCPv6 pool with an interface, only that pool services requests on the associated interface. The pool also services other interfaces. If you do not associate a DHCPv6 pool with an interface, it can service requests on any interface.

Not using any IPv6 address prefix means that the pool returns only configured options.

The link-address command allows matching a link-address without necessarily allocating an address. You can match the pool from multiple relays by using multiple link-address configuration commands inside a pool.

Since a longest match is performed on either the address pool information or the link information, you can configure one pool to allocate addresses and another pool on a subprefix that returns only configured options.

### Examples

The following example specifies a DHCP for IPv6 configuration information pool named cisco1 and places the router in DHCP for IPv6 pool configuration mode:

```
Device(config)# ipv6 dhcp pool cisco1
Device(config-dhcpv6)#
```

The following example shows how to configure an IPv6 address prefix for the IPv6 configuration pool cisco1:

```
Device(config-dhcpv6)# address prefix 2001:1000::0/64
Device(config-dhcpv6)# end
```

The following example shows how to configure a pool named engineering with three link-address prefixes and an IPv6 address prefix:

```
Device# configure terminal
Device(config)# ipv6 dhcp pool engineering
Device(config-dhcpv6)# link-address 2001:1001::0/64
Device(config-dhcpv6)# link-address 2001:1002::0/64
Device(config-dhcpv6)# link-address 2001:2000::0/48
Device(config-dhcpv6)# address prefix 2001:1003::0/64
Device(config-dhcpv6)# end
```

The following example shows how to configure a pool named 350 with vendor-specific options:

```
Device# configure terminal
Device(config)# ipv6 dhcp pool 350
Device(config-dhcpv6)# vendor-specific 9
Device(config-dhcpv6-vs)# suboption 1 address 1000:235D::1
Device(config-dhcpv6-vs)# suboption 2 ascii "IP-Phone"
Device(config-dhcpv6-vs)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp server</td>
<td>Enables DHCP for IPv6 service on an interface.</td>
</tr>
<tr>
<td>show ipv6 dhcp pool</td>
<td>Displays DHCP for IPv6 configuration pool information.</td>
</tr>
</tbody>
</table>
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.

**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**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

- `ipv6-monitor-name`: Activates a previously created flow monitor by assigning it to the interface to analyze incoming or outgoing traffic.
- `sampler ipv6-sampler-name`: Applies the flow monitor sampler.
- `input`: Applies the flow monitor on input traffic.
- `output`: Applies the flow monitor on output traffic.

**Command Default**

IPv6 flow monitor is not activated until it is assigned to an interface.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot attach a NetFlow monitor to a port channel interface. If both service module interfaces are part of an EtherChannel, you should attach the monitor to both physical interfaces.

This example shows how to apply a flow monitor to an interface:

```
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-2 output
Device(config-if)# end
```
ipv6 general-prefix

To define an IPv6 general prefix, use the `ipv6 general-prefix` command in global configuration mode. To remove the IPv6 general prefix, use the `no` form of this command.

```
ipv6 general-prefix prefix-name {ipv6-prefix/prefix-length | 6to4 interface-type interface-number | 6rd interface-type interface-number}
no ipv6 general-prefix prefix-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>prefix-name</code></td>
<td>The name assigned to the prefix.</td>
</tr>
<tr>
<td><code>ipv6-prefix</code></td>
<td>The IPv6 network assigned to the general prefix.</td>
</tr>
<tr>
<td></td>
<td>This argument must be in the form documented in RFC 2373 where the address is</td>
</tr>
<tr>
<td></td>
<td>specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td></td>
<td>When defining a general prefix manually, specify both the <code>ipv6-prefix</code> and /</td>
</tr>
<tr>
<td></td>
<td><code>prefix-length</code> arguments.</td>
</tr>
<tr>
<td><code>/ prefix-length</code></td>
<td>The length of the IPv6 prefix. A decimal value that indicates how many of the</td>
</tr>
<tr>
<td></td>
<td>high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td></td>
<td>When defining a general prefix manually, specify both the <code>ipv6-prefix</code> and /</td>
</tr>
<tr>
<td></td>
<td><code>prefix-length</code> arguments.</td>
</tr>
<tr>
<td><code>6to4</code></td>
<td>Allows configuration of a general prefix based on an interface used for 6to4 tunneling.</td>
</tr>
<tr>
<td></td>
<td>When defining a general prefix based on a 6to4 interface, specify the <code>6to4</code> keyword and the <code>interface-type interface-number</code> argument.</td>
</tr>
<tr>
<td><code>interface-type interface-number</code></td>
<td>Interface type and number. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td></td>
<td>When defining a general prefix based on a 6to4 interface, specify the <code>6to4</code> keyword and the <code>interface-type interface-number</code> argument.</td>
</tr>
<tr>
<td><code>6rd</code></td>
<td>Allows configuration of a general prefix computed from an interface used for IPv6 rapid deployment (6RD) tunneling.</td>
</tr>
</tbody>
</table>

**Command Default**

No general prefix is defined.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the ipv6 general-prefix command to define an IPv6 general prefix.
A general prefix holds a short prefix, based on which a number of longer, more specific, prefixes can be defined. When the general prefix is changed, all of the more specific prefixes based on it will change, too. This function greatly simplifies network renumbering and allows for automated prefix definition.

More specific prefixes, based on a general prefix, can be used when configuring IPv6 on an interface.

When defining a general prefix based on an interface used for 6to4 tunneling, the general prefix will be of the form 2002:a.b.c.d::/48, where "a.b.c.d" is the IPv4 address of the interface referenced.

**Examples**

The following example manually defines an IPv6 general prefix named my-prefix:

```
Device(config)# ipv6 general-prefix my-prefix 2001:DB8:2222::/48
```

The following example defines an IPv6 general prefix named my-prefix based on a 6to4 interface:

```
Device(config)# ipv6 general-prefix my-prefix 6to4 ethernet0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 general-prefix</td>
<td>Displays information on general prefixes for an IPv6 addresses.</td>
</tr>
</tbody>
</table>
ipv6 local policy route-map

To enable local policy-based routing (PBR) for IPv6 packets, use the `ipv6 local policy route-map` command in global configuration mode. To disable local policy-based routing for IPv6 packets, use the `no` form of this command.

```
ipv6 local policy route-map route-map-name
no ipv6 local policy route-map route-map-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>route-map-name</code></td>
<td>Name of the route map to be used for local IPv6 PBR. The name must match a <code>route-map-name</code> value specified by the <code>route-map</code> command.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv6 packets are not policy routed.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Packets originating from a router are not normally policy routed. However, you can use the `ipv6 local policy route-map` command to policy route such packets. You might enable local PBR if you want packets originated at the router to take a route other than the obvious shortest path.

The `ipv6 local policy route-map` command identifies a route map to be used for local PBR. The `route-map` commands each have a list of `match` and `set` commands associated with them. The `match` commands specify the match criteria, which are the conditions under which packets should be policy routed. The `set` commands specify set actions, which are particular policy routing actions to be performed if the criteria enforced by the `match` commands are met. The `no ipv6 local policy route-map` command deletes the reference to the route map and disables local policy routing.

**Examples**

In the following example, packets with a destination IPv6 address matching that allowed by access list `pbr-src-90` are sent to the router at IPv6 address `2001:DB8::1`:

```
ipv6 access-list src-90
    permit ipv6 host 2001::90 2001:1000::/64
route-map pbr-src-90 permit 10
    match ipv6 address src-90
    set ipv6 next-hop 2001:DB8::1
ipv6 local policy route-map pbr-src-90
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 policy route-map</code></td>
<td>Configures IPv6 PBR on an interface.</td>
</tr>
<tr>
<td><code>match ipv6 address</code></td>
<td>Specifies an IPv6 access list to be used to match packets for PBR for IPv6.</td>
</tr>
<tr>
<td><code>match length</code></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set default interface</td>
<td>Specifies the default interface to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.</td>
</tr>
<tr>
<td>set interface</td>
<td>Specifies the default interface to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>set ipv6 default next-hop</td>
<td>Specifies an IPv6 default next hop to which matching packets will be forwarded.</td>
</tr>
<tr>
<td>set ipv6 next-hop (PBR)</td>
<td>Indicates where to output IPv6 packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td>set ipv6 precedence</td>
<td>Sets the precedence value in the IPv6 packet header.</td>
</tr>
</tbody>
</table>
ipv6 local pool

To configure a local IPv6 prefix pool, use the ipv6 local pool configuration command with the prefix pool name. To disband the pool, use the no form of this command.

```plaintext
ipv6 local pool poolname prefix/prefix-length assigned-length [shared] [cache-size size]
no ipv6 local pool poolname
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>poolname</strong></td>
<td>User-defined name for the local prefix pool.</td>
</tr>
<tr>
<td><strong>prefix</strong></td>
<td>IPv6 prefix assigned to the pool.</td>
</tr>
<tr>
<td><strong>prefix-length</strong></td>
<td>This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td><strong>assigned-length</strong></td>
<td>The length of the IPv6 prefix assigned to the pool. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address).</td>
</tr>
<tr>
<td><strong>shared</strong></td>
<td>Length of prefix, in bits, assigned to the user from the pool. The value of the assigned-length argument cannot be less than the value of the \prefix-length argument.</td>
</tr>
<tr>
<td><strong>cache-size size</strong></td>
<td>(Optional) Indicates that the pool is a shared pool.</td>
</tr>
</tbody>
</table>

**Command Default**

No pool is configured.

**Command Modes**

Global configuration (global)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All pool names must be unique.

IPv6 prefix pools have a function similar to IPv4 address pools. Contrary to IPv4, a block of addresses (an address prefix) are assigned and not single addresses.

Prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, the pool must be removed and recreated. All prefixes already allocated will also be freed.

**Examples**

This example shows the creation of an IPv6 prefix pool:

```plaintext
Device(config)# ipv6 local pool pool1 2001:0DB8::/29 64
Device(config)# end
Device# show ipv6 local pool
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 pool</code></td>
<td>Enables IPv6 pool debugging.</td>
</tr>
<tr>
<td><code>peer default ipv6 address pool</code></td>
<td>Specifies the pool from which client prefixes are assigned for PPP links.</td>
</tr>
<tr>
<td><code>prefix-delegation pool</code></td>
<td>Specifies a named IPv6 local prefix pool from which prefixes are delegated to DHCP for IPv6 clients.</td>
</tr>
<tr>
<td><code>show ipv6 local pool</code></td>
<td>Displays information about any defined IPv6 address pools.</td>
</tr>
</tbody>
</table>
ipv6 mld snooping

To enable Multicast Listener Discovery version 2 (MLDv2) protocol snooping globally, use the `ipv6 mld snooping` command in global configuration mode. To disable the MLDv2 snooping globally, use the `no` form of this command.

```
ipv6 mld snooping
no ipv6 mld snooping
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

This command is enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced on the Supervisor Engine 720.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

MLDv2 snooping is supported on the Supervisor Engine 720 with all versions of the Policy Feature Card 3 (PFC3).

To use MLDv2 snooping, configure a Layer 3 interface in the subnet for IPv6 multicast routing or enable the MLDv2 snooping querier in the subnet.

**Examples**

This example shows how to enable MLDv2 snooping globally:

```
Device(config)# ipv6 mld snooping
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 mld snooping</code></td>
<td>Displays MLDv2 snooping information.</td>
</tr>
</tbody>
</table>
**ipv6 mld ssm-map enable**

To enable the Source Specific Multicast (SSM) mapping feature for groups in the configured SSM range, use the `ipv6 mld ssm-map enable` command in global configuration mode. To disable this feature, use the `no` form of this command.

```
ipv6 mld [vrf vrf-name] ssm-map enable
no ipv6 mld [vrf vrf-name] ssm-map enable
```

**Syntax Description**

<table>
<thead>
<tr>
<th>vrf</th>
<th>vrf-name (Optional) Specifies a virtual routing and forwarding (VRF) configuration.</th>
</tr>
</thead>
</table>

**Command Default**

The SSM mapping feature is not enabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 mld ssm-map enable` command enables the SSM mapping feature for groups in the configured SSM range. When the `ipv6 mld ssm-map enable` command is used, SSM mapping defaults to use the Domain Name System (DNS).

SSM mapping is applied only to received Multicast Listener Discovery (MLD) version 1 or MLD version 2 membership reports.

**Examples**

The following example shows how to enable the SSM mapping feature:

```
Device(config)# ipv6 mld ssm-map enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 mld ssm-map</code></td>
<td>Displays debug messages for SSM mapping.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map query dns</code></td>
<td>Enables DNS-based SSM mapping.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map static</code></td>
<td>Configures static SSM mappings.</td>
</tr>
<tr>
<td><code>show ipv6 mld ssm-map</code></td>
<td>Displays SSM mapping information.</td>
</tr>
</tbody>
</table>
ipv6 mld state-limit

To limit the number of Multicast Listener Discovery (MLD) states globally, use the `ipv6 mld state-limit` command in global configuration mode. To disable a configured MLD state limit, use the `no` form of this command.

```
ipv6 mld [vrf vrf-name] state-limit number
no ipv6 mld [vrf vrf-name] state-limit number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Maximum number of MLD states allowed on a router. The valid range is from 1 to 64000.</td>
</tr>
</tbody>
</table>

**Command Default**

No default number of MLD limits is configured. You must configure the number of maximum MLD states allowed globally on a router when you configure this command.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 mld state-limit` command to configure a limit on the number of MLD states resulting from MLD membership reports on a global basis. Membership reports sent after the configured limits have been exceeded are not entered in the MLD cache and traffic for the excess membership reports is not forwarded.

Use the `ipv6 mld limit` command in interface configuration mode to configure the per-interface MLD state limit.

Per-interface and per-system limits operate independently of each other and can enforce different configured limits. A membership state will be ignored if it exceeds either the per-interface limit or global limit.

**Examples**

The following example shows how to limit the number of MLD states on a router to 300:

```
Device(config)# ipv6 mld state-limit 300
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mld access-group</code></td>
<td>Enables the performance of IPv6 multicast receiver access control.</td>
</tr>
<tr>
<td><code>ipv6 mld limit</code></td>
<td>Limits the number of MLD states resulting from MLD membership state on a per-interface basis.</td>
</tr>
</tbody>
</table>
ipv6 multicast-routing

To enable multicast routing using Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router and to enable multicast forwarding, use the `ipv6 multicast-routing` command in global configuration mode. To stop multicast routing and forwarding, use the `no` form of this command.

```
ipv6 multicast-routing [vrf vrf-name]
no ipv6 multicast-routing
```

Syntax Description

- **vrf vrf-name**: (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Multicast routing is not enabled.

Command Modes

- Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `ipv6 multicast-routing` command to enable multicast forwarding. This command also enables Protocol Independent Multicast (PIM) and Multicast Listener Discovery (MLD) on all IPv6-enabled interfaces of the router being configured.

You can configure individual interfaces before you enable multicast so that you can then explicitly disable PIM and MLD protocol processing on those interfaces, as needed. Use the `no ipv6 pim` or the `no ipv6 mld router` command to disable IPv6 PIM or MLD router-side processing, respectively.

Examples

The following example enables multicast routing and turns on PIM and MLD on all interfaces:

```
Device(config)# ipv6 multicast-routing
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim rp-address</td>
<td>Configures the address of a PIM RP for a particular group range.</td>
</tr>
<tr>
<td>no ipv6 pim</td>
<td>Turns off IPv6 PIM on a specified interface.</td>
</tr>
<tr>
<td>no ipv6 mld router</td>
<td>Disables MLD router-side processing on a specified interface.</td>
</tr>
</tbody>
</table>
ipv6 multicast group-range

To disable multicast protocol actions and traffic forwarding for unauthorized groups or channels on all the interfaces in a router, use the `ipv6 multicast group-range` command in global configuration mode. To return to the command’s default settings, use the `no` form of this command.

```
ipv6 multicast [vrf vrf-name] group-range [access-list-name]
no ipv6 multicast [vrf vrf-name] group-range [access-list-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>access-list-name</td>
<td>(Optional) Name of an access list that contains authenticated subscriber groups and authorized channels that can send traffic to the router.</td>
</tr>
</tbody>
</table>

**Command Default**

Multicast is enabled for groups and channels permitted by a specified access list and disabled for groups and channels denied by a specified access list.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 multicast group-range` command provides an access control mechanism for IPv6 multicast edge routing. The access list specified by the `access-list-name` argument specifies the multicast groups or channels that are to be permitted or denied. For denied groups or channels, the router ignores protocol traffic and actions (for example, no Multicast Listener Discovery (MLD) states are created, no mroute states are created, no Protocol Independent Multicast (PIM) joins are forwarded), and drops data traffic on all interfaces in the system, thus disabling multicast for denied groups or channels.

Using the `ipv6 multicast group-range` global configuration command is equivalent to configuring the MLD access control and multicast boundary commands on all interfaces in the system. However, the `ipv6 multicast group-range` command can be overridden on selected interfaces by using the following interface configuration commands:

- `ipv6 mld access-group access-list-name`
- `ipv6 multicast boundary scope scope-value`

Because the `no ipv6 multicast group-range` command returns the router to its default configuration, existing multicast deployments are not broken.

**Examples**

The following example ensures that the router disables multicast for groups or channels denied by an access list named list2:

```
Device(config)# ipv6 multicast group-range list2
```

The following example shows that the command in the previous example is overridden on an interface specified by int2:

```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group list2
```
Device(config)# interface int2
Device(config-if)# ipv6 mld access-group int-list2

On int2, MLD states are created for groups or channels permitted by int-list2 but are not created for groups or channels denied by int-list2. On all other interfaces, the access-list named list2 is used for access control.

In this example, list2 can be specified to deny all or most multicast groups or channels, and int-list2 can be specified to permit authorized groups or channels only for interface int2.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld access-group</td>
<td>Performs IPv6 multicast receiver access control.</td>
</tr>
<tr>
<td>ipv6 multicast boundary</td>
<td>Configures a multicast boundary on the interface for a specified scope.</td>
</tr>
</tbody>
</table>
ipv6 multicast pim-passive-enable

To enable the Protocol Independent Multicast (PIM) passive feature on an IPv6 router, use the **ipv6 multicast pim-passive-enable** command in global configuration mode. To disable this feature, use the **no** form of this command.

```
ipv6 multicast pim-passive-enable
no ipv6 multicast pim-passive-enable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

PIM passive mode is not enabled on the router.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **ipv6 multicast pim-passive-enable** command to configure IPv6 PIM passive mode on a router. Once PIM passive mode is configured globally, use the **ipv6 pim passive** command in interface configuration mode to configure PIM passive mode on a specific interface.

**Examples**

The following example configures IPv6 PIM passive mode on a router:

```
Device(config)# ipv6 multicast pim-passive-enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim passive</td>
<td>Configures PIM passive mode on a specific interface.</td>
</tr>
</tbody>
</table>
ipv6 multicast rpf

To enable IPv6 multicast reverse path forwarding (RPF) check to use Border Gateway Protocol (BGP) unicast routes in the Routing Information Base (RIB), use the `ipv6 multicast rpf` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ipv6 multicast [vrf vrf-name] rpf {backoff initial-delay max-delay | use-bgp}
no ipv6 multicast [vrf vrf-name] rpf {backoff initial-delay max-delay | use-bgp}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td><code>backoff</code></td>
<td>Specifies the backoff delay after a unicast routing change.</td>
</tr>
<tr>
<td><code>initial-delay</code></td>
<td>Initial RPF backoff delay, in milliseconds (ms). The range is from 200 to 65535.</td>
</tr>
<tr>
<td><code>max-delay</code></td>
<td>Maximum RPF backoff delay, in ms. The range is from 200 to 65535.</td>
</tr>
<tr>
<td><code>use-bgp</code></td>
<td>Specifies to use BGP routes for multicast RPF lookups.</td>
</tr>
</tbody>
</table>

**Command Default**

The multicast RPF check does not use BGP unicast routes.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `ipv6 multicast rpf` command is configured, multicast RPF check uses BGP unicast routes in the RIB. This is not done by default.

**Examples**

The following example shows how to enable the multicast RPF check function:

```
Device(config)# ipv6 multicast rpf use-bgp
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast limit</code></td>
<td>Configure per-interface multicast route (mroute) state limiters in IPv6.</td>
</tr>
<tr>
<td><code>ipv6 multicast multipath</code></td>
<td>Enables load splitting of IPv6 multicast traffic across multiple equal-cost paths.</td>
</tr>
</tbody>
</table>
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**

- `expire-time-in-seconds` (Optional) 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced for the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd na glean</code></td>
<td>Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.</td>
</tr>
<tr>
<td><code>ipv6 nd nud retry</code></td>
<td>Configures the number of times neighbor unreachability detection resends neighbor solicitations.</td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays the usability status of interfaces that are configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 nd cache interface-limit (global)

To configure a neighbor discovery cache limit on all interfaces on the device, use the **ipv6 nd cache interface-limit** command in global configuration mode. To remove the neighbor discovery from all interfaces on the device, use the **no** form of this command.

```
ipv6 nd cache interface-limit size [log rate]
no ipv6 nd cache interface-limit size [log rate]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>size</strong></td>
</tr>
<tr>
<td><strong>log rate</strong></td>
</tr>
</tbody>
</table>

**Command Default**

Default logging rate for the device is one entry every second.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ipv6 nd cache interface-limit** command in global configuration mode imposes a common per-interface cache size limit on all interfaces on the device.

Issuing the **no** or default form of the command will remove the neighbor discovery limit from every interface on the device that was configured using global configuration mode. It will not remove the neighbor discovery limit from any interface configured using the **ipv6 nd cache interface-limit** command in interface configuration mode.

The default (and maximum) logging rate for the device is one entry every second.

**Examples**

The following example shows how to set a common per-interface cache size limit of 4 seconds on all interfaces on the device:

```
Device(config)# ipv6 nd cache interface-limit 4
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv6 nd cache interface-limit (interface)</strong></td>
<td>Configures a neighbor discovery cache limit on a specified interface on the device.</td>
</tr>
</tbody>
</table>
ipv6 nd host mode strict

To enable the conformant, or strict, IPv6 host mode, use the `ipv6 nd host mode strict` command in global configuration mode. To reenable conformant, or loose, IPv6 host mode, use the no form of this command.

```
ipv6 nd host mode strict
```

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

**Command Default**
Nonconformant, or loose, IPv6 host mode is enabled.

**Command Modes**
Global configuration (config)

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The default IPv6 host mode type is loose, or nonconformant. To enable IPv6 strict, or conformant, host mode, use the `ipv6 nd host mode strict` command. You can change between the two IPv6 host modes using the no form of this command.

The `ipv6 nd host mode strict` command selects the type of IPv6 host mode behavior and enters interface configuration mode. However, the `ipv6 nd host mode strict` command is ignored if you have configured IPv6 routing with the `ipv6 unicast-routing` command. In this situation, the default IPv6 host mode type, loose, is used.

**Examples**
The following example shows how to configure the device as a strict IPv6 host and enables IPv6 address autoconfiguration on Ethernet interface 0/0:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address autoconfig
```

The following example shows how to configure the device as a strict IPv6 host and configures a static IPv6 address on Ethernet interface 0/0:

```
Device(config)# ipv6 nd host mode strict
Device(config-if)# interface ethernet0/0
Device(config-if)# ipv6 address 2001::1/64
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enables the forwarding of IPv6 unicast datagrams.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Command History</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd cache expire</code></td>
<td>Configures the duration of time before an IPv6 neighbor discovery cache entry expires.</td>
</tr>
<tr>
<td><code>ipv6 nd nud retry</code></td>
<td>Configures the number of times neighbor unreachability detection resends neighbor solicitations.</td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays the usability status of interfaces that are configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation (NS) retransmissions on an interface, use the `ipv6 nd ns-interval` command in interface configuration mode. To restore the default interval, use the `no` form of this command.

```
ipv6 nd ns-interval milliseconds
no ipv6 nd ns-interval
```

**Syntax Description**

| milliseconds | The interval between IPv6 neighbor solicit transmissions for address resolution. The acceptable range is from 1000 to 3600000 milliseconds. |

**Command Default**

0 milliseconds (unspecified) is advertised in router advertisements and the value 1000 is used for the neighbor discovery activity of the router itself.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By default, using the `ipv6 nd ns-interval` command changes the NS retransmission interval for both address resolution and duplicate address detection (DAD). To specify a different NS retransmission interval for DAD, use the `ipv6 nd dad time` command.

This value will be included in all IPv6 router advertisements sent out this interface. Very short intervals are not recommended in normal IPv6 operation. When a nondefault value is configured, the configured time is both advertised and used by the router itself.

**Examples**

The following example configures an IPv6 neighbor solicit transmission interval of 9000 milliseconds for Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd ns-interval 9000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd dad time</td>
<td>Configures the NS retransmit interval for DAD separately from the NS retransmit interval for address resolution.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>base</code></td>
<td>The neighbor unreachability detection process base value.</td>
</tr>
<tr>
<td><code>interval</code></td>
<td>The time interval, in milliseconds, between retries.</td>
</tr>
<tr>
<td></td>
<td>The range is from 1000 to 32000.</td>
</tr>
<tr>
<td><code>max-attempts</code></td>
<td>The maximum number of retry attempts, depending on the base value.</td>
</tr>
<tr>
<td></td>
<td>The range is from 1 to 128.</td>
</tr>
<tr>
<td><code>final-wait-time</code></td>
<td>The waiting time, in milliseconds, on the last probe.</td>
</tr>
<tr>
<td></td>
<td>The range is from 1000 to 32000.</td>
</tr>
</tbody>
</table>

### Command Modes

- Interface configuration (config-if)

### Command History

- **Release**
  - Cisco IOS XE Everest 16.5.1a
- **Modification**
  - This command was introduced for the Cisco Catalyst 9500 Series Switches.

### 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 unreachable 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 nd cache expire</code></td>
<td>Configures the duration of time before an IPv6 neighbor discovery (ND) cache entry expires.</td>
</tr>
<tr>
<td><code>ipv6 nd na glean</code></td>
<td>Configures neighbor discovery to glean an entry from an unsolicited neighbor advertisement.</td>
</tr>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays the usability status of interfaces that are configured for IPv6.</td>
</tr>
</tbody>
</table>
ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after some reachability confirmation event has occurred, use the ipv6 nd reachable-time command in interface configuration mode. To restore the default time, use the no form of this command.

```
ipv6 nd reachable-time milliseconds
no ipv6 nd reachable-time
```

**Syntax Description**

| milliseconds | The amount of time that a remote IPv6 node is considered reachable (in milliseconds). |

**Command Default**

0 milliseconds (unspecified) is advertised in router advertisements and the value 30000 (30 seconds) is used for the neighbor discovery activity of the router itself.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The configured time enables the router to detect unavailable neighbors. Shorter configured times enable the router to detect unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

The configured time is included in all router advertisements sent out of an interface so that nodes on the same link use the same time value. A value of 0 means indicates that the configured time is unspecified by this router.

**Examples**

The following example configures an IPv6 reachable time of 1,700,000 milliseconds for Ethernet interface 0/0:

```
Device(config)# interface ethernet 0/0
Device(config-if)# ipv6 nd reachable-time 1700000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 interface</td>
<td>Displays the usability status of interfaces configured for IPv6.</td>
</tr>
</tbody>
</table>
**ipv6 nd resolution data limit**

To configure the number of data packets queued pending Neighbor Discovery resolution, use the `ipv6 nd resolution data limit` command in global configuration mode.

```
ipv6 nd resolution data limit number-of-packets
no ipv6 nd resolution data limit number-of-packets
```

**Syntax Description**

- `number-of-packets` - The number of queued data packets. The range is from 16 to 2048 packets.

**Command Default**

Queue limit is 16 packets.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd resolution data limit` command allows the customer to configure the number of data packets queued pending Neighbor Discovery resolution. IPv6 Neighbor Discovery queues a data packet that initiates resolution for an unresolved destination. Neighbor Discovery will only queue one packet per destination. Neighbor Discovery also enforces a global (per-router) limit on the number of packets queued. Once the global queue limit is reached, further packets to unresolved destinations are discarded. The minimum (and default) value is 16 packets, and the maximum value is 2048.

In most situations, the default value of 16 queued packets pending Neighbor Discovery resolution is sufficient. However, in some high-scalability scenarios in which the router needs to initiate communication with a very large number of neighbors almost simultaneously, then the value may be insufficient. This may lead to loss of the initial packet sent to some neighbors. In most applications, the initial packet is retransmitted, so initial packet loss generally is not a cause for concern. (Note that dropping the initial packet to an unresolved destination is normal in IPv4.) However, there may be some high-scale configurations where loss of the initial packet is inconvenient. In these cases, the customer can use the `ipv6 nd resolution data limit` command to prevent the initial packet loss by increasing the unresolved packet queue size.

**Examples**

The following example configures the global number of data packets held awaiting resolution to be 32:

```
Device(config)# ipv6 nd resolution data limit 32
```
ipv6 nd route-owner

To insert Neighbor Discovery-learned routes into the routing table with "ND" status and to enable ND autoconfiguration behavior, use the `ipv6 nd route-owner` command. To remove this information from the routing table, use the `no` form of this command.

```
ipv6   ndroute-owner
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The status of Neighbor Discovery-learned routes is "Static."

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 nd route-owner` command inserts routes learned by Neighbor Discovery into the routing table with a status of "ND" rather than "Static" or "Connected."

This global command also enables you to use the `ipv6 nd autoconfig default` or `ipv6 nd autoconfig prefix` commands in interface configuration mode. If the `ipv6 nd route-owner` command is not issued, then the `ipv6 nd autoconfig default` and `ipv6 nd autoconfig prefix` commands are accepted by the router but will not work.

**Examples**

```
Device(config)# ipv6 nd route-owner
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd autoconfig default</td>
<td>Allows Neighbor Discovery to install a default route to the Neighbor Discovery-derived default router.</td>
</tr>
<tr>
<td>ipv6 nd autoconfig prefix</td>
<td>Uses Neighbor Discovery to install all valid on-link prefixes from RAs received on the interface.</td>
</tr>
</tbody>
</table>
### ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the `ipv6 neighbor` command in global configuration mode. To remove a static IPv6 entry from the IPv6 neighbor discovery cache, use the `no` form of this command.

```
ipv6 neighbor ipv6-address interface-type interface-number hardware-address
no ipv6 neighbor ipv6-address interface-type interface-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6-address</code></td>
<td>The IPv6 address that corresponds to the local data-link address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>The specified interface type. For supported interface types, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>The specified interface number.</td>
</tr>
<tr>
<td><code>hardware-address</code></td>
<td>The local data-link address (a 48-bit address).</td>
</tr>
</tbody>
</table>

**Command Default**

Static entries are not configured in the IPv6 neighbor discovery cache.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 neighbor` command is similar to the `arp` (global) command.

If an entry for the specified IPv6 address already exists in the neighbor discovery cache--learned through the IPv6 neighbor discovery process--the entry is automatically converted to a static entry.

Use the `show ipv6 neighbors` command to view static entries in the IPv6 neighbor discovery cache. A static entry in the IPv6 neighbor discovery cache can have one of the following states:

- INCMP (Incomplete)--The interface for this entry is down.
- REACH (Reachable)--The interface for this entry is up.

**Note**

Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP and REACH states are different for dynamic and static cache entries. See the `show ipv6 neighbors` command for descriptions of the INCMP and REACH states for dynamic cache entries.

The `clear ipv6 neighbors` command deletes all entries in the IPv6 neighbor discovery cache, except static entries. The `no ipv6 neighbor` command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries--learned from the IPv6 neighbor discovery process--from the
cache. Disabling IPv6 on an interface by using the `no ipv6 enable` command or the `no ipv6 unnumbered` command deletes all IPv6 neighbor discovery cache entries configured for that interface, except static entries (the state of the entry changes to INCMP).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

**Note**
Static entries for IPv6 neighbors can be configured only on IPv6-enabled LAN and ATM LAN Emulation interfaces.

**Examples**

The following example configures a static entry in the IPv6 neighbor discovery cache for a neighbor with the IPv6 address 2001:0DB8::45A and link-layer address 0002.7D1A.9472 on Ethernet interface 1:

```
Device(config)# ipv6 neighbor 2001:0DB8::45A ethernet1 0002.7D1A.9472
```
**ipv6 ospf name-lookup**

To display Open Shortest Path First (OSPF) router IDs as Domain Naming System (DNS) names, use the `ipv6 ospf name-lookup` command in global configuration mode. To stop displaying OSPF router IDs as DNS names, use the `no` form of this command.

```
ipv6 ospf name-lookup
no ipv6 ospf name-lookup
```

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

**Command Default**
This command is disabled by default.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

**Examples**
The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
Device(config)# ipv6 ospf name-lookup
```

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the `ipv6 pim` command in interface configuration mode. To disable PIM on a specified interface, use the `no` form of the command.

```
ipv6 pim
no ipv6 pim
```

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

**Command Default**
PIM is automatically enabled on every interface.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
After a user has enabled the `ipv6 multicast-routing` command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the `no` form of the `ipv6 pim` command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

**Examples**
The following example turns off PIM on Fast Ethernet interface 1/0:

```
Device(config)# interface FastEthernet 1/0
Device(config-if)# no ipv6 pim
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 multicast-routing</code></td>
<td>Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.</td>
</tr>
</tbody>
</table>
ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the `ipv6 pim accept-register` command in global configuration mode. To return to the default value, use the `no` form of this command.

```
ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
no ipv6 pim [vrf vrf-name] accept-register {list access-list | route-map map-name}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>list access-list</td>
<td>Defines the access list name.</td>
</tr>
<tr>
<td>route-map map-name</td>
<td>Defines the route map.</td>
</tr>
</tbody>
</table>

**Command Default**

All sources are accepted at the RP.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 pim accept-register` command to configure a named access list or route map with match attributes. When the permit conditions as defined by the `access-list` and `map-name` arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

**Examples**

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
match as-path 101
ip as-path access-list 101 permit
```
ipv6 pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv6 device, use the `ip pim allow-rp` command in global configuration mode. To return to the default value, use the `no` form of this command.

```
ipv6 pim allow-rp [{group-list access-list | rp-list access-list [group-list access-list]}]
no ipv6 pim allow-rp
```

Syntax Description

- `group-list`: (Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.
- `rp-list`: (Optional) Specifies an ACL for allowed rendezvous-point (RP) addresses for PIM Allow RP.
- `access-list`: (Optional) Unique number or name of a standard ACL.

Command Default

PIM Allow RP is disabled.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to enable the receiving device in an IP multicast network to accept a (*, G) Join from an unexpected (different) RP address.

Before enabling PIM Allow RP, you must first use the `ipv6 pim rp-address` command to define an RP.

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim rp-address</td>
<td>S Marco:configure the address of a PIM RP for multicast groups.</td>
</tr>
</tbody>
</table>
**ipv6 pim neighbor-filter list**

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the `ipv6 pim neighbor-filter list` command in the global configuration mode. To return to the router default, use the `no` form of this command.

```
ipv6 pim [vrf vrf-name] neighbor-filter list access-list
no ipv6 pim [vrf vrf-name] neighbor-filter list access-list
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.
- `access-list` Name of an IPv6 access list that denies PIM hello packets from a source.

**Command Default**

PIM neighbor messages are not filtered.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ipv6 pim neighbor-filter list` command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

**Examples**

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
Device(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Device(config)# ipv6 access-list nbr_filter_acl
Device(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Device(config-ipv6-acl)# permit any any
```
ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the `ipv6 pim rp-address` command in global configuration mode. To remove an RP address, use the `no` form of this command.

```
ipv6 pim [vrf vrf-name] rp-address ipv6-address [group-access-list] [bidir]
no ipv6 pim rp-address ipv6-address [group-access-list] [bidir]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>vrf vrf-name</th>
<th>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6-address</td>
<td>The IPv6 address of a router to be a PIM RP.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The <code>ipv6-address</code> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td></td>
<td>group-access-list</td>
<td>(Optional) Name of an access list that defines for which multicast groups the RP should be used.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range (FF3x::/96), a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).</td>
</tr>
<tr>
<td></td>
<td>bidir</td>
<td>(Optional) Indicates that the group range will be used for bidirectional shared-tree forwarding; otherwise, it will be used for sparse-mode forwarding. A single IPv6 address can be configured to be RP only for either bidirectional or sparse-mode group ranges.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A single group-range list can be configured to operate either in bidirectional or sparse mode.</td>
</tr>
</tbody>
</table>

**Command Default**

No PIM RPs are preconfigured. Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided). Multicast groups operate in PIM sparse mode.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1aCisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router.

Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will
discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional `group-access-list` argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-7]:/8 to FF3X::/96. If the `group-access-list` argument is specified, the IPv6 address is the RP address for the group range specified in the `group-access-list` argument.

You can configure Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

### Examples

The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
Device(config) # ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Device(config) # ipv6 access-list acc-grp-1
Device(config-ipv6-acl) # permit ipv6 any ff04::/64
Device(config) # ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Device(config) # ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
Device(config) # ipv6 access-list embd-ranges
Device(config-ipv6-acl) # permit ipv6 any ff73:240:2:2:2::/96
Device(config-ipv6-acl) # permit ipv6 any ff74:240:2:2:2::/96
Device(config-ipv6-acl) # permit ipv6 any ff75:240:2:2:2::/96
Device(config-ipv6-acl) # permit ipv6 any ff76:240:2:2:2::/96
Device(config-ipv6-acl) # permit ipv6 any ff77:240:2:2:2::/96
Device(config-ipv6-acl) # permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Device(config) # ipv6 access-list bidir-grps
Device(config-ipv6-acl) # permit ipv6 any ff05::/16
Device(config-ipv6-acl) # permit ipv6 any ff06::/16
Device(config-ipv6-acl) # exit
Device(config) # ipv6 pim rp-address 200::1 bidir-grps bidir
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug ipv6 pim df-election</td>
<td>Displays debug messages for PIM bidirectional DF-election message processing.</td>
</tr>
<tr>
<td>ipv6 access-list</td>
<td>Defines an IPv6 access list and places the router in IPv6 access list configuration mode.</td>
</tr>
<tr>
<td>show ipv6 pim df</td>
<td>Displays the DF-election state of each interface for each RP.</td>
</tr>
<tr>
<td>show ipv6 pim df winner</td>
<td>Displays the DF-election winner on each interface for each RP.</td>
</tr>
</tbody>
</table>
**ipv6 pim rp embedded**

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the `ipv6 pim rp-embedded` command in global configuration mode. To disable embedded RP support, use the `no` form of this command.

```
ipv6 pim [vrf vrf-name] rp embedded
no ipv6 pim [vrf vrf-name] rp embedded
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Default**

Embedded RP support is enabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Because embedded RP support is enabled by default, users will generally use the `no` form of this command to turn off embedded RP support.

The `ipv6 pim rp embedded` command applies only to the embedded RP group ranges ff7X::/16 and ff1X::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and ff1X::/16, and extracts the RP to be used from the group address.

**Examples**

The following example disables embedded RP support in IPv6 PIM:

```
Device# no ipv6 pim rp embedded
```
**ipv6 pim spt-threshold infinity**

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the `ipv6 pim spt-threshold infinity` command in global configuration mode. To restore the default value, use the `no` form of this command.

```
ipv6 pim [vrf vrf-name] spt-threshold infinity [group-list access-list-name]
no ipv6 pim spt-threshold infinity
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.
- `group-list access-list-name` (Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups.

**Command Default**

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the `ipv6 pim spt-threshold infinity` command will not cause it to switch to the shared tree.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Using the `ipv6 pim spt-threshold infinity` command enables all sources for the specified groups to use the shared tree. The `group-list` keyword indicates to which groups the SPT threshold applies.

The `access-list-name` argument refers to an IPv6 access list. When the `access-list-name` argument is specified with a value of 0, or the `group-list` keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

**Examples**

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group range ff04::/64:

```
Device(config)# ipv6 access-list acc-grp-1
Device(config-ipv6-acl)# permit ipv6 any FF04::/64
Device(config-ipv6-acl)# exit
Device(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```
**ipv6 prefix-list**

To create an entry in an IPv6 prefix list, use the `ipv6 prefix-list` command in global configuration mode. To delete the entry, use the `no` form of this command.

```plaintext
ipv6 prefix-list list-name [seq seq-number] {deny ipv6-prefix/prefix-length | permit ipv6-prefix/prefix-length | description text} [ge ge-value] [le le-value]
no ipv6 prefix-list list-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>Name of the prefix list.</td>
</tr>
<tr>
<td>seq seq-number</td>
<td>(Optional) Sequence number of the prefix list entry being configured.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies networks that matches the condition.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits networks that matches the condition.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>The IPv6 network assigned to the specified prefix list. This argument must</td>
</tr>
<tr>
<td></td>
<td>be in the form documented in RFC 2373 where the address is specified in</td>
</tr>
<tr>
<td></td>
<td>hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>The length of the IPv6 prefix. A decimal value that indicates how many of</td>
</tr>
<tr>
<td></td>
<td>the high-order contiguous bits of the address comprise the prefix (the</td>
</tr>
<tr>
<td></td>
<td>network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td>description text</td>
<td>A description of the prefix list that can be up to 80 characters in length.</td>
</tr>
<tr>
<td>ge ge-value</td>
<td>(Optional) Specifies a prefix length greater than or equal to the ipv6-prefix/prefix-length arguments. It is the lowest value of a range of the length (the “from” portion of the length range).</td>
</tr>
<tr>
<td>le le-value</td>
<td>(Optional) Specifies a prefix length less than or equal to the ipv6-prefix/prefix-length arguments. It is the highest value of a range of the length (the “to” portion of the length range).</td>
</tr>
</tbody>
</table>

**Command Default**

No prefix list is created.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
The **ipv6 prefix-list** command is similar to the **ip prefix-list** command, except that it is IPv6-specific.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

The sequence number of a prefix list entry determines the order of the entries in the list. The router compares network addresses to the prefix list entries. The router begins the comparison at the top of the prefix list, with the entry having the lowest sequence number.

If multiple entries of a prefix list match a prefix, the entry with the lowest sequence number is considered the real match. Once a match or deny occurs, the router does not go through the rest of the prefix list. For efficiency, you may want to put the most common permits or denies near the top of the list, using the **seq-number** argument.

The **show ipv6 prefix-list** command displays the sequence numbers of entries.

IPv6 prefix lists are used to specify certain prefixes or a range of prefixes that must be matched before a permit or deny statement can be applied. Two operand keywords can be used to designate a range of prefix lengths to be matched. A prefix length of less than, or equal to, a value is configured with the **le** keyword. A prefix length greater than, or equal to, a value is specified using the **ge** keyword. The **ge** and **le** keywords can be used to specify the range of the prefix length to be matched in more detail than the usual **ipv6-prefix/prefix-length** argument. For a candidate prefix to match against a prefix list entry three conditions can exist:

- The candidate prefix must match the specified prefix list and prefix length entry.
- The value of the optional **le** keyword specifies the range of allowed prefix lengths from the **prefix-length** argument up to, and including, the value of the **le** keyword.
- The value of the optional **ge** keyword specifies the range of allowed prefix lengths from the value of the **ge** keyword up to, and including, 128.

The first condition must match before the other conditions take effect.

An exact match is assumed when the **ge** or **le** keywords are not specified. If only one keyword operand is specified then the condition for that keyword is applied, and the other condition is not applied. The **prefix-length** value must be less than the **ge** value. The **ge** value must be less than, or equal to, the **le** value. The **le** value must be less than or equal to 128.

Every IPv6 prefix list, including prefix lists that do not have any permit and deny condition statements, has an implicit deny any statement as its last match condition.

**Examples**

The following example denies all routes with a prefix of ::/0.

```
Device(config)# ipv6 prefix-list abc deny ::/0
```

The following example permits the prefix 2002::/16:

```
Device(config)# ipv6 prefix-list abc permit 2002::/16
```

The following example shows how to specify a group of prefixes to accept any prefixes from prefix 5F00::/48 up to and including prefix 5F00::/64.

```
Device(config)# ipv6 prefix-list abc permit 5F00::/48 le 64
```
The following example denies prefix lengths greater than 64 bits in routes that have the prefix 2001:0DB8::/64.

```
Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
```

The following example permits mask lengths from 32 to 64 bits in all address space.

```
Device(config)# ipv6 prefix-list abc permit ::/0 ge 32 le 64
```

The following example denies mask lengths greater than 32 bits in all address space.

```
Device(config)# ipv6 prefix-list abc deny ::/0 ge 32
```

The following example denies all routes with a prefix of 2002::/128.

```
Device(config)# ipv6 prefix-list abc deny 2002::/128
```

The following example permits all routes with a prefix of ::/0.

```
Device(config)# ipv6 prefix-list abc permit ::/0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 prefix-list</td>
<td>Resets the hit count of the IPv6 prefix list entries.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ipv6 prefix-list sequence-number</td>
<td>Enables the generation of sequence numbers for entries in an IPv6 prefix list.</td>
</tr>
<tr>
<td>match ipv6 address</td>
<td>Distributes IPv6 routes that have a prefix permitted by a prefix list.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Displays information about an IPv6 prefix list or IPv6 prefix list entries.</td>
</tr>
</tbody>
</table>
ipv6 source-guard attach-policy

To apply IPv6 source guard policy on an interface, use the `ipv6 source-guard attach-policy` in interface configuration mode. To remove this source guard from the interface, use the `no` form of this command.

```
ipv6 source-guard attach-policy [source-guard-policy]
```

**Syntax Description**

- `source-guard-policy` (Optional) User-defined name of the source guard policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

**Command Default**

An IPv6 source-guard policy is not applied on the interface.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no policy is specified using the `source-guard-policy` argument, then the default source-guard policy is applied.

A dependency exists between IPv6 source guard and IPv6 snooping. Whenever IPv6 source guard is configured, when the `ipv6 source-guard attach-policy` command is entered, it verifies that snooping is enabled and issues a warning if it is not. If IPv6 snooping is disabled, the software checks if IPv6 source guard is enabled and sends a warning if it is.

**Examples**

The following example shows how to apply IPv6 source guard on an interface:

```
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# ipv6 source-guard attach-policy mysnoopingpolicy
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 snooping policy</code></td>
<td>Configures an IPv6 snooping policy and enters IPv6 snooping configuration mode.</td>
</tr>
</tbody>
</table>
ipv6 source-route

To enable processing of the IPv6 type 0 routing header (the IPv6 source routing header), use the `ipv6 source-route` command in global configuration mode. To disable the processing of this IPv6 extension header, use the `no` form of this command.

```
ipv6 source-route
no ipv6 source-route
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The `no` version of the `ipv6 source-route` command is the default. When the router receives a packet with a type 0 routing header, the router drops the packet and sends an IPv6 Internet Control Message Protocol (ICMP) error message back to the source and logs an appropriate debug message.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default was changed to be the `no` version of the `ipv6 source-route` command, which means this functionality is not enabled. Before this change, this functionality was enabled automatically. User who had configured the `no ipv6 source-route` command before the default was changed will continue to see this configuration in their `show config` command output, even though the `no` version of the command is the default.

The `no ipv6 source-route` command (which is the default) prevents hosts from performing source routing using your routers. When the `no ipv6 source-route` command is configured and the router receives a packet with a type0 source routing header, the router drops the packet and sends an IPv6 ICMP error message back to the source and logs an appropriate debug message.

In IPv6, source routing is performed only by the destination of the packet. Therefore, in order to stop source routing from occurring inside your network, you need to configure an IPv6 access control list (ACL) that includes the following rule:

```
deny ipv6 any any routing
```

The rate at which the router generates all IPv6 ICMP error messages can be limited by using the `ipv6 icmp error-interval` command.

**Examples**

The following example disables the processing of IPv6 type 0 routing headers:

```
no ipv6 source-route
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny (IPv6)</code></td>
<td>Sets deny conditions for an IPv6 access list.</td>
</tr>
<tr>
<td><code>ipv6 icmp error-interval</code></td>
<td>Configures the interval for IPv6 ICMP error messages.</td>
</tr>
</tbody>
</table>
**ipv6 spd mode**

To configure an IPv6 Selective Packet Discard (SPD) mode, use the `ipv6 spd mode` command in global configuration mode. To remove the IPv6 SPD mode, use the `no` form of this command.

```
ipv6 spd mode {aggressive | tos protocol ospf}
no ipv6 spd mode {aggressive | tos protocol ospf}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggressive</td>
<td>Aggressive drop mode discards incorrectly formatted packets when the IPv6 SPD is in random drop state.</td>
</tr>
<tr>
<td>tos protocol ospf</td>
<td>OSPF mode allows OSPF packets to be handled with SPD priority.</td>
</tr>
</tbody>
</table>

**Command Default**

No IPv6 SPD mode is configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default setting for the IPv6 SPD mode is none, but you may want to use the `ipv6 spd mode` command to configure a mode to be used when a certain SPD state is reached.

The `aggressive` keyword enables aggressive drop mode, which drops deformed packets when IPv6 SPD is in random drop state. The `ospf` keyword enables OSPF mode, in which OSPF packets are handled with SPD priority.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

**Examples**

The following example shows how to enable the router to drop deformed packets when the router is in the random drop state:

```
Device(config)# ipv6 spd mode aggressive
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 spd queue max-threshold</td>
<td>Configures the maximum number of packets in the IPv6 SPD process input queue.</td>
</tr>
<tr>
<td>ipv6 spd queue min-threshold</td>
<td>Configures the minimum number of packets in the IPv6 SPD process input queue.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>show ipv6 spd</td>
<td>Displays the IPv6 SPD configuration.</td>
</tr>
</tbody>
</table>
ipv6 spd queue max-threshold

To configure the maximum number of packets in the IPv6 Selective Packet Discard (SPD) process input queue, use the `ipv6 spd queue max-threshold` command in global configuration mode. To return to the default value, use the `no` form of this command.

```
ipv6 spd queue max-threshold value
no ipv6 spd queue max-threshold
```

**Syntax Description**

| `value` | Number of packets. The range is from 0 through 65535. |

**Command Default**

No SPD queue maximum threshold value is configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ipv6 spd queue max-threshold` command to configure the SPD queue maximum threshold value.

The size of the process input queue governs the SPD state: normal (no drop), random drop, or max. When the process input queue is less than the SPD minimum threshold, SPD takes no action and enters normal state. In the normal state, no packets are dropped. When the input queue reaches the maximum threshold, SPD enters max state, in which normal priority packets are discarded. If the input queue is between the minimum and maximum thresholds, SPD enters the random drop state, in which normal packets may be dropped.

**Examples**

The following example shows how to set the maximum threshold value of the queue to 60,000:

```
Device(config)# ipv6 spd queue max-threshold 60000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 spd queue min-threshold</td>
<td>Configures the minimum number of packets in the IPv6 SPD process input queue.</td>
</tr>
<tr>
<td>show ipv6 spd</td>
<td>Displays the IPv6 SPD configuration.</td>
</tr>
</tbody>
</table>
**ipv6 traffic interface-statistics**

To collect IPv6 forwarding statistics for all interfaces, use the `ipv6 traffic interface-statistics` command in global configuration mode. To ensure that IPv6 forwarding statistics are not collected for any interface, use the `no` form of this command.

```
ipv6 traffic interface-statistics [unclearable]
no ipv6 traffic interface-statistics [unclearable]
```

### Syntax Description

| **unclearable** | (Optional) IPv6 forwarding statistics are kept for all interfaces, but it is not possible to clear the statistics on any interface. |

### Command Default

IPv6 forwarding statistics are collected for all interfaces.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Using the optional `unclearable` keyword halves the per-interface statistics storage requirements.

### Examples

The following example does not allow statistics to be cleared on any interface:

```
Device(config)# ipv6 traffic interface-statistics unclearable
```
ipv6 unicast-routing

To enable the forwarding of IPv6 unicast datagrams, use the ipv6 unicast-routing command in global configuration mode. To disable the forwarding of IPv6 unicast datagrams, use the no form of this command.

```
ipv6 unicast-routing
no ipv6 unicast-routing
```

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

**Command Default**
IPv6 unicast routing is disabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Configuring the no ipv6 unicast-routing command removes all IPv6 routing protocol entries from the IPv6 routing table.

**Examples**
The following example enables the forwarding of IPv6 unicast datagrams:

```
Device(config)# ipv6 unicast-routing
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 address link-local</td>
<td>Configures an IPv6 link-local address for an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td>ipv6 address eui-64</td>
<td>Configures an IPv6 address and enables IPv6 processing on an interface using an EUI-64 interface ID in the low-order 64 bits of the address.</td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>Enables IPv6 processing on an interface that has not been configured with an explicit IPv6 address.</td>
</tr>
<tr>
<td>ipv6 unnumbered</td>
<td>Enables IPv6 processing on an interface without assigning an explicit IPv6 address to the interface.</td>
</tr>
<tr>
<td>show ipv6 route</td>
<td>Displays the current contents of the IPv6 routing table.</td>
</tr>
</tbody>
</table>
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**

| name-of-chain | 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>accept-lifetime</strong></td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td><strong>key</strong></td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td><strong>key-string (authentication)</strong></td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td><strong>send-lifetime</strong></td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td><strong>show key chain</strong></td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Text</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>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.</td>
</tr>
</tbody>
</table>

## 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Defines an authentication key-chain needed to enable authentication for routing protocols.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td>show key chain</td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
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**
- `key-id`: 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 Modes**
- Key-chain configuration (config-keychain)

**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**
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept-lifetime</code></td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td><code>key chain</code></td>
<td>Defines an authentication key chain needed to enable authentication for routing protocols.</td>
</tr>
<tr>
<td><code>key-string (authentication)</code></td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td><code>send-lifetime</code></td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
<tr>
<td><code>show key chain</code></td>
<td>Displays authentication key information.</td>
</tr>
</tbody>
</table>
**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}]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed NHS information.</td>
</tr>
<tr>
<td><code>redundancy</code></td>
<td>(Optional) Displays information about NHS redundancy stacks.</td>
</tr>
<tr>
<td><code>cluster number</code></td>
<td>(Optional) Displays redundancy cluster information.</td>
</tr>
<tr>
<td><code>preempted</code></td>
<td>(Optional) Displays information about NHS that failed to become active and is preempted.</td>
</tr>
<tr>
<td><code>running</code></td>
<td>(Optional) Displays NHSs that are currently in Responding or Expecting replies states.</td>
</tr>
<tr>
<td><code>waiting</code></td>
<td>(Optional) Displays NHSs awaiting to be scheduled.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The table below lists the valid types, number ranges, and descriptions for the optional `interface` argument.

The valid types can vary according to the platform and interfaces on the platform.

**Table 18: Valid Types, Number Ranges, and Interface Descriptions**

<table>
<thead>
<tr>
<th>Valid Types</th>
<th>Number Ranges</th>
<th>Interface Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANI</td>
<td>0 to 1000</td>
<td>Autonomic-Networking virtual interface</td>
</tr>
<tr>
<td>Auto-Template</td>
<td>1 to 999</td>
<td>Auto-Template interface</td>
</tr>
<tr>
<td>GMPLS</td>
<td>0 to 1000</td>
<td>Multiprotocol Label Switching (MPLS) interface</td>
</tr>
<tr>
<td>GigabitEthernet</td>
<td>0 to 9</td>
<td>GigabitEthernet IEEE 802.3z</td>
</tr>
</tbody>
</table>
### Interface Descriptions

<table>
<thead>
<tr>
<th>Valid Types</th>
<th>Number Ranges</th>
<th>Interface Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Interface</td>
<td>0 to 9</td>
<td>Internal interface</td>
</tr>
<tr>
<td>LISP</td>
<td>0 to 65520</td>
<td>Locator/ID Separation Protocol (LISP) virtual interface</td>
</tr>
<tr>
<td>loopback</td>
<td>0 to 2147483647</td>
<td>Loopback interface</td>
</tr>
<tr>
<td>Null</td>
<td>0 to 0</td>
<td>Null interface</td>
</tr>
<tr>
<td>PROTECTION_GROUP</td>
<td>0 to 0</td>
<td>Protection-group controller</td>
</tr>
<tr>
<td>Port-channel</td>
<td>1 to 128</td>
<td>Port channel interface</td>
</tr>
<tr>
<td>TenGigabitEthernet</td>
<td>0 to 9</td>
<td>TenGigabitEthernet interface</td>
</tr>
<tr>
<td>Tunnel</td>
<td>0 to 2147483647</td>
<td>Tunnel interface</td>
</tr>
<tr>
<td>Tunnel-tp</td>
<td>0 to 65535</td>
<td>MPLS Transport Profile interface</td>
</tr>
<tr>
<td>Vlan</td>
<td>1 to 4094</td>
<td>VLAN interface</td>
</tr>
</tbody>
</table>

### 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
Tunnel1:
    10.1.1.1    E  req-sent 128  req-failed 1  repl-recev 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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel1</td>
<td>Interface through which the target network is reached.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip nhrp map</code></td>
<td>Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.</td>
</tr>
<tr>
<td><code>show ip nhrp</code></td>
<td>Displays NHRP mapping information.</td>
</tr>
</tbody>
</table>
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command provides a list of all open TCP/IP ports on the system including the ports opened using Cisco networking stack.

To close open ports, you can use one of the following methods:

- Use Access Control List (ACL).
- To close the UDP 2228 port, use the `no l2 traceroute` command.
- To close TCP 80, TCP 443, TCP 6970, TCP 8090 ports, use the `no ip http server` and `no ip http secure-server` commands.

**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 *:* O/[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 20: Field Descriptions of show ip ports all**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Transport protocol used.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
Local Address. | Device IP Address.
Foreign Address | Remote or peer address.
State | State of the connection. It can be listen, established or connected.
PID/Program Name | Process ID or name

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show tcp brief all</strong></td>
<td>Displays information about TCP connection endpoints.</td>
</tr>
<tr>
<td><strong>show ip sockets</strong></td>
<td>Displays IP sockets information.</td>
</tr>
</tbody>
</table>
show ipv6 access-list

To display the contents of all current IPv6 access lists, use the `show ipv6 access-list` command in user EXEC or privileged EXEC mode.

`show ipv6 access-list [access-list-name]`

**Syntax Description**

| access-list-name | (Optional) Name of access list. |

**Command Default**

All IPv6 access lists are displayed.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 access-list` command provides output similar to the `show ip access-list` command, except that it is IPv6-specific.

**Examples**

The following output from the `show ipv6 access-list` command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Device# show ipv6 access-list
IPv6 access list inbound
   permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
   permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
   permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
   permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time left 243) sequence 1
   permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300 (time left 296) sequence 2
IPv6 access list outbound
   evaluate udptraffic
   evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Device# show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
   permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
   permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.
Table 21: show ipv6 access-list Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 access list inbound</td>
<td>Name of the IPv6 access list, for example, inbound.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits any packet that matches the specified protocol type.</td>
</tr>
<tr>
<td>tcp</td>
<td>Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.</td>
</tr>
<tr>
<td>any</td>
<td>Equal to ::/0.</td>
</tr>
<tr>
<td>eq</td>
<td>An equal operand that compares the source or destination ports of TCP or UDP packets.</td>
</tr>
<tr>
<td>bgp</td>
<td>Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.</td>
</tr>
<tr>
<td>reflect</td>
<td>Indicates a reflexive IPv6 access list.</td>
</tr>
<tr>
<td>tcptraffic (8 matches)</td>
<td>The name of the reflexive IPv6 access list and the number of matches for the access list. The clear ipv6 access-list privileged EXEC command resets the IPv6 access list match counters.</td>
</tr>
<tr>
<td>sequence 10</td>
<td>Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).</td>
</tr>
<tr>
<td>host 2001:0DB8:1::1</td>
<td>The source IPv6 host address that the source address of the packet must match.</td>
</tr>
<tr>
<td>host 2001:0DB8:1::2</td>
<td>The destination IPv6 host address that the destination address of the packet must match.</td>
</tr>
<tr>
<td>11000</td>
<td>The ephemeral source port number for the outgoing connection.</td>
</tr>
<tr>
<td>timeout 300</td>
<td>The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.</td>
</tr>
<tr>
<td>(time left 243)</td>
<td>The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.</td>
</tr>
<tr>
<td>evaluate udptraffic</td>
<td>Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 access-list</td>
<td>Resets the IPv6 access list match counters.</td>
</tr>
<tr>
<td>hardware statistics</td>
<td>Enables the collection of hardware statistics.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays the contents of all current IP access lists.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
<tr>
<td>show ipv6 prefix-list</td>
<td>Displays information about an IPv6 prefix list or IPv6 prefix list entries.</td>
</tr>
</tbody>
</table>
show ipv6 destination-guard policy

To display destination guard information, use the show ipv6 destination-guard policy command in privileged EXEC mode.

show ipv6 destination-guard policy [policy-name]

Syntax Description

| policy-name | (Optional) Name of the destination guard policy. |

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If the policy-name argument is specified, only the specified policy information is displayed. If the policy-name argument is not specified, information is displayed for all policies.

Examples

The following is sample output from the show ipv6 destination-guard policy command when the policy is applied to a VLAN:

Device# show ipv6 destination-guard policy poll
Destination guard policy destination:
  enforcement always
  Target: vlan 300

The following is sample output from the show ipv6 destination-guard policy command when the policy is applied to an interface:

Device# show ipv6 destination-guard policy poll
Destination guard policy destination:
  enforcement always
  Target: Gi0/0/1

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 destination-guard policy</td>
<td>Defines the destination guard policy.</td>
</tr>
</tbody>
</table>
**show ipv6 dhcp**

To display the Dynamic Host Configuration Protocol (DHCP) unique identifier (DUID) on a specified device, use the `show ipv6 dhcp` command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.3.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 dhcp` command uses the DUID based on the link-layer address for both client and server identifiers. The device uses the MAC address from the lowest-numbered interface to form the DUID. The network interface is assumed to be permanently attached to the device. Use the `show ipv6 dhcp` command to display the DUID of a device.

**Examples**

The following is sample output from the `show ipv6 dhcp` command. The output is self-explanatory:

```
Device# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 000300010002FCA5DC1C
```
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**
- `ipv6-address` (Optional) The address of a DHCP for IPv6 client.
- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**
- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 0x0000C0001, 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 0x0000D0001, T1 75, T2 135
    Prefix: 2001:0DB8:E00::/64
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The table below describes the significant fields shown in the display.

**Table 22: show ipv6 dhcp binding Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>Address of a specified client.</td>
</tr>
<tr>
<td>DUID</td>
<td>DHCP unique identifier (DUID).</td>
</tr>
<tr>
<td>Virtual-Access2.1</td>
<td>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.</td>
</tr>
<tr>
<td>Username : client_1</td>
<td>The username associated with the binding.</td>
</tr>
<tr>
<td>IA PD</td>
<td>Collection of prefixes assigned to a client.</td>
</tr>
<tr>
<td>IA ID</td>
<td>Identifier for this IAPD.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Prefixes delegated to the indicated IAPD on the specified client.</td>
</tr>
<tr>
<td>preferred lifetime, valid lifetime</td>
<td>The preferred lifetime and valid lifetime settings, in seconds, for the specified client.</td>
</tr>
<tr>
<td>Expires at</td>
<td>Date and time at which the valid lifetime expires.</td>
</tr>
<tr>
<td>Virtual-Access2.2</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 is 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:FEBB:CC
        DUID: 0003000100AA00BB00CC
        Username : unassigned
        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)
```
Device# show ipv6 dhcp binding

Client: FE80::2AA:FF:FEBB:CC
DUID: 0003000100AA00BB00CC
Username: unassigned
Interface: Virtual-Access2
IA PD: IA ID 0x00130001, T1 150, T2 240
  Prefix: 2001:0DB8:1:v0::/60
  preferred lifetime 300, valid lifetime 300
  expires at Aug 11 2008 06:23 AM (233 seconds)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp server vrf enable</td>
<td>Enables the DHCPv6 server VRF-aware feature.</td>
</tr>
<tr>
<td>clear ipv6 dhcp binding</td>
<td>Deletes automatic client bindings from the DHCP for IPv6 binding table.</td>
</tr>
</tbody>
</table>
**show ipv6 dhcp conflict**

To display address conflicts found by a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server when addresses are offered to the client, use the `show ipv6 dhcp conflict` command in privileged EXEC mode.

```
show ipv6 dhcp conflict [ipv6-address] [vrf vrf-name]
```

**Syntax Description**
- `ipv6-address` (Optional) The address of a DHCP for IPv6 client.
- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>Cisco IOS XE Everest 16.5.1a</td>
</tr>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you configure the DHCPv6 server to detect conflicts, it uses ping. The client uses neighbor discovery to detect clients and reports to the server through a DECLINE message. If an address conflict is detected, the address is removed from the pool, and the address is not assigned until the administrator removes the address from the conflict list.

**Examples**

The following is a sample output from the `show ipv6 dhcp conflict` command. This command shows the pool and prefix values for DHCP conflicts:

```
Device# show ipv6 dhcp conflict
Pool 350, prefix 2001:0DB8:1005::/48
   2001:0DB8:1005::10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp conflict</td>
<td>Clears an address conflict from the DHCPv6 server database.</td>
</tr>
</tbody>
</table>
**show ipv6 dhcp database**

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the `show ipv6 dhcp database` command in user EXEC or privileged EXEC mode.

**show ipv6 dhcp database [agent-URL]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>agent-URL</th>
<th>(Optional) A flash, NVRAM, FTP, TFTP, or remote copy protocol (RCP) uniform resource locator.</th>
</tr>
</thead>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Each permanent storage to which the binding database is saved is called the database agent. An agent can be configured using the `ipv6 dhcp database` command. Supported database agents include FTP and TFTP servers, RCP, Flash file system, and NVRAM.

The `show ipv6 dhcp database` command displays DHCP for IPv6 binding database agent information. If the `agent-URL` argument is specified, only the specified agent is displayed. If the `agent-URL` argument is not specified, all database agents are shown.

**Examples**

The following is sample output from the `show ipv6 dhcp database` command:

```
Device# show ipv6 dhcp database
Database agent tftp://172.19.216.133/db.tftp:
  write delay: 69 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
  write timer expires in 56 seconds
  last read at Jan 06 2003 05:41 PM
  successful read times 1
  failed read times 0
  successful write times 3172
  failed write times 2
Database agent nvram:/dhcpv6-binding:
  write delay: 60 seconds, transfer timeout: 300 seconds
  last written at Jan 09 2003 01:54 PM,
  write timer expires in 37 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 3325
  failed write times 0
Database agent flash:/dhcpv6-db:
  write delay: 82 seconds, transfer timeout: 3 seconds
  last written at Jan 09 2003 01:54 PM,
  write timer expires in 50 seconds
  last read at never
```
The table below describes the significant fields shown in the display.

### Table 23: show ipv6 dhcp database Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database agent</td>
<td>Specifies the database agent.</td>
</tr>
<tr>
<td>Write delay</td>
<td>The amount of time (in seconds) to wait before updating the database.</td>
</tr>
<tr>
<td>transfer timeout</td>
<td>Specifies how long (in seconds) the DHCP server should wait before aborting a database transfer. Transfers that exceed the timeout period are aborted.</td>
</tr>
<tr>
<td>Last written</td>
<td>The last date and time bindings were written to the file server.</td>
</tr>
<tr>
<td>Write timer expires...</td>
<td>The length of time, in seconds, before the write timer expires.</td>
</tr>
<tr>
<td>Last read</td>
<td>The last date and time bindings were read from the file server.</td>
</tr>
<tr>
<td>Successful/failed read times</td>
<td>The number of successful or failed read times.</td>
</tr>
<tr>
<td>Successful/failed write times</td>
<td>The number of successful or failed write times.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp database</td>
<td>Specifies DHCP for IPv6 binding database agent parameters.</td>
</tr>
</tbody>
</table>
show ipv6 dhcp guard policy

To display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) guard information, use the **show ipv6 dhcp guard policy** command in privileged EXEC mode.

**show ipv6 dhcp guard policy [policy-name]**

**Syntax Description**

| policy-name | (Optional) DHCPv6 guard policy name.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `policy-name` argument is specified, only the specified policy information is displayed. If the `policy-name` argument is not specified, information is displayed for all policies.

**Examples**

The following is sample output from the **show ipv6 dhcp guard guard** command:

```
Device# show ipv6 dhcp guard policy

Dhcp guard policy: default
  Device Role: dhcp client
  Target: Et0/3

Dhcp guard policy: test1
  Device Role: dhcp server
  Target: vlan 0  vlan 1  vlan 2  vlan 3  vlan 4
  Max Preference: 200
  Min Preference: 0
  Source Address Match Access List: acl1
  Prefix List Match Prefix List: pfxlist1

Dhcp guard policy: test2
  Device Role: dhcp relay
  Target: Et0/0 Et0/1 Et0/2
```

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

**Table 24: show ipv6 dhcp guard Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Role</td>
<td>The role of the device. The role is either client, server or relay.</td>
</tr>
<tr>
<td>Target</td>
<td>The name of the target. The target is either an interface or a VLAN.</td>
</tr>
</tbody>
</table>
show ipv6 dhcp guard policy

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 dhcp guard policy</td>
<td>Defines the DHCPv6 guard policy name.</td>
</tr>
</tbody>
</table>
**show ipv6 dhcp interface**

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the `show ipv6 dhcp interface` command in user EXEC or privileged EXEC mode.

**Syntax Description**

```
show ipv6 dhcp interface [type number]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>type number</th>
<th>(Optional) Interface type and number. For more information, use the question mark (?) online help function.</th>
</tr>
</thead>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If no interfaces are specified, all interfaces on which DHCP for IPv6 (client or server) is enabled are shown. If an interface is specified, only information about the specified interface is displayed.

**Examples**

The following is sample output from the `show ipv6 dhcp interface` command. In the first example, the command is used on a router that has an interface acting as a DHCP for IPv6 server. In the second example, the command is used on a router that has an interface acting as a DHCP for IPv6 client:

```
Device# show ipv6 dhcp interface
Ethernet2/1 is in server mode
  Using pool: svr-p1
  Preference value: 20
  Rapid-Commit is disabled
Router2# show ipv6 dhcp interface
Ethernet2/1 is in client mode
  State is OPEN (1)
  List of known servers:
    Address: FE80::202:FCFF:FEA1:7439, DUID 000300010002FCA17400
    Preference: 20
    IA PD: IA ID 0x00040001, T1 120, T2 192
      Prefix: 3FFE:C00:C18:1::/72
        preferred lifetime 240, valid lifetime 54321
        expires at Nov 08 2002 09:10 AM (54319 seconds)
      Prefix: 3FFE:C00:C18:2::/72
        preferred lifetime 300, valid lifetime 54333
        expires at Nov 08 2002 09:11 AM (54331 seconds)
      Prefix: 3FFE:C00:C18:3::/72
        preferred lifetime 280, valid lifetime 51111
        expires at Nov 08 2002 08:17 AM (51109 seconds)
    DNS server: 1001::1
    DNS server: 1001::2
    Domain name: domain1.net
    Domain name: domain2.net
    Domain name: domain3.net
```

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**

463
Prefix name is cli-p1
Rapid-Commit is enabled

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

Table 25: show ipv6 dhcp interface Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet2/1 is in server/client mode</td>
<td>Displays whether the specified interface is in server or client mode.</td>
</tr>
<tr>
<td>Preference value:</td>
<td>The advertised (or default of 0) preference value for the indicated server.</td>
</tr>
<tr>
<td>Prefix name is cli-p1</td>
<td>Displays the IPv6 general prefix pool name, in which prefixes successfully acquired on this interface are stored.</td>
</tr>
<tr>
<td>Using pool: svr-p1</td>
<td>The name of the pool that is being used by the interface.</td>
</tr>
<tr>
<td>State is OPEN</td>
<td>State of the DHCP for IPv6 client on this interface. &quot;Open&quot; indicates that configuration information has been received.</td>
</tr>
<tr>
<td>List of known servers</td>
<td>Lists the servers on the interface.</td>
</tr>
<tr>
<td>Address, DUID</td>
<td>Address and DHCP unique identifier (DUID) of a server heard on the specified interface.</td>
</tr>
<tr>
<td>Rapid commit is disabled</td>
<td>Displays whether the rapid-commit keyword has been enabled on the interface.</td>
</tr>
</tbody>
</table>

The following example shows the DHCP for IPv6 relay agent configuration on FastEthernet interface 0/0, and use of the show ipv6 dhcp interface command displays relay agent information on FastEthernet interface 0/0:

```
Device(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 FastEthernet0/1
Device# show ipv6 dhcp interface FastEthernet 0/0
FastEthernet0/0 is in relay mode
    Relay destinations:
        FE80::250:A2FF:FEBF:A056 via FastEthernet0/1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 dhcp client pd</td>
<td>Enables the DHCP for IPv6 client process and enables requests for prefix delegation through a specified interface.</td>
</tr>
<tr>
<td>ipv6 dhcp relay destination</td>
<td>Specifies a destination address to which client messages are forwarded and enables DHCP for IPv6 relay service on the interface.</td>
</tr>
<tr>
<td>ipv6 dhcp server</td>
<td>Enables DHCP for IPv6 service on an interface.</td>
</tr>
</tbody>
</table>
show ipv6 dhcp relay binding

To display DHCPv6 Internet Assigned Numbers Authority (IANA) and DHCPv6 Identity Association for Prefix Delegation (IAPD) bindings on a relay agent, use the `show ipv6 dhcp relay binding` command in user EXEC or privileged EXEC mode.

```
show ipv6 dhcp relay binding [vrf vrf-name]
```

**Syntax Description**
- **vrf vrf-name** (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**
- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `vrf vrf-name` keyword-argument pair is specified, all bindings belonging to the specified VRF are displayed.

**Note**

Only the DHCPv6 IAPD bindings on a relay agent are displayed on the Cisco uBR10012 and Cisco uBR7200 series universal broadband devices.

**Examples**

The following is sample output from the `show ipv6 dhcp relay binding` command:

```
Device# show ipv6 dhcp relay binding
```

The following example shows output from the `show ipv6 dhcp relay binding` command with a specified VRF name on a Cisco uBR10012 universal broadband device:

```
Device# show ipv6 dhcp relay binding vrf vrf1
Prefix: 2001:DB8:0:1::/64 (Bundle100.600)
 DUID: 000300010023B6D94D31
 IAID: 3201912114
 lifetime: 600
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix</td>
<td>IPv6 prefix for DHCP.</td>
</tr>
</tbody>
</table>
### show ipv6 dhcp relay binding

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DUID</td>
<td>DHCP Unique Identifier (DUID) for the IPv6 relay binding.</td>
</tr>
<tr>
<td>IAID</td>
<td>Identity Association Identification (IAID) for DHCP.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Lifetime of the prefix, in seconds.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 dhcp relay binding</td>
<td>Clears a specific IPv6 address or IPv6 prefix of a DHCP for IPv6 relay binding.</td>
</tr>
<tr>
<td>debug ipv6 dhcp relay</td>
<td>Enables debugging for IPv6 DHCP relay agent.</td>
</tr>
<tr>
<td>debug ipv6 dhcp relay bulk-lease</td>
<td>Enables bulk lease query debugging for IPv6 DHCP relay agent.</td>
</tr>
</tbody>
</table>
show ipv6 eigrp events

To display Enhanced Interior Gateway Routing Protocol (EIGRP) events logged for IPv6, use the `show ipv6 eigrp events` command in user EXEC or privileged EXEC mode.

```
show ipv6 eigrp events [errmsg | sia] [event-num-start event-num-end] | type]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errmsg</code></td>
<td>(Optional) Displays error messages being logged.</td>
</tr>
<tr>
<td><code>sia</code></td>
<td>(Optional) Displays Stuck In Active (SIA) messages.</td>
</tr>
<tr>
<td><code>event-num-start</code></td>
<td>(Optional) Starting number of the event range. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td><code>event-num-end</code></td>
<td>(Optional) Ending number of the event range. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td><code>type</code></td>
<td>(Optional) Displays event types being logged.</td>
</tr>
</tbody>
</table>

**Command Default**

If no event range is specified, information for all IPv6 EIGRP events is displayed.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 eigrp events` command is used to analyze a network failure by the Cisco support team and is not intended for general use. This command provides internal state information about EIGRP and how it processes route notifications and changes.

**Examples**

The following is sample output from the `show ipv6 eigrp events` command. The fields are self-explanatory.

```
Device# show ipv6 eigrp events
Event information for AS 65535:
  1 00:56:41.719 State change: Successor Origin Local origin
  2 00:56:41.719 Metric set: 2555:5555::/32 4294967295
  3 00:56:41.719 Poison squashed: 2555:5555::/32 lost if
  4 00:56:41.719 Poison squashed: 2555:5555::/32 rt gone
  5 00:56:41.719 Route installing: 2555:5555::/32 FE80::ABCD:4:EF00:1
  6 00:56:41.719 RDB delete: 2555:5555::/32 FE80::ABCD:4:EF00:2
  7 00:56:41.719 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:1
  8 00:56:41.719 Find FS: 2555:5555::/32 4294967295
  9 00:56:41.719 Free reply status: 2555:5555::/32
 10 00:56:41.719 Clr handle num/bits: 0 0x0
 11 00:56:41.719 Clr handle dest/cnt: 2555:5555::/32 0
 12 00:56:41.719 Rcv reply met/succ met: 4294967295 4294967295
 13 00:56:41.719 Rcv reply dest/nh: 2555:5555::/32 FE80::ABCD:4:EF00:2
 14 00:56:41.687 Send reply: 2555:5555::/32 FE80::ABCD:4:EF00:2
 15 00:56:41.687 Rcv query met/succ met: 4294967295 4294967295
```
show ipv6 eigrp events

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 eigrp</td>
<td>Deletes entries from EIGRP for IPv6 routing tables.</td>
</tr>
<tr>
<td>debug ipv6 eigrp</td>
<td>Displays information about EIGRP for IPv6 protocol.</td>
</tr>
<tr>
<td>ipv6 eigrp</td>
<td>Enables EIGRP for IPv6 on a specified interface.</td>
</tr>
</tbody>
</table>

Related Commands
show ipv6 eigrp interfaces

To display information about interfaces configured for the Enhanced Interior Gateway Routing Protocol (EIGRP) in IPv6 topologies, use the show ipv6 eigrp interfaces command in user EXEC or privileged EXEC mode.

show ipv6 eigrp [as-number] interfaces [type number] [detail]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>(Optional) Autonomous system number.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed interface information.</td>
</tr>
</tbody>
</table>

Command Modes

- User EXEC (>)
- Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the show ipv6 eigrp interfaces command to determine the interfaces on which EIGRP is active and to get information about EIGRP processes related to those interfaces. The optional type number argument and the detail keyword can be entered in any order.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the show ipv6 eigrp interfaces command:

```
Device# show ipv6 eigrp 1 interfaces
IPv6-EIGRP interfaces for process 1
Interface    Peers  Un/Reliable  Xmit Queue  Mean  Pacing Time  Multicast  Pending
Et0/0         0       0/0/0        0/10       0/0/0/0  0/10        0/0/0/0
```

The following is sample output from the show ipv6 eigrp interfaces detail command:

```
Device# show ipv6 eigrp interfaces detail
IPv6-EIGRP interfaces for process 1
Interface    Peers  Un/Reliable  Xmit Queue  Mean  Pacing Time  Multicast  Pending
Et0/0         0       0/0/0        0/10       0/0/0/0  0/10        0/0/0/0
```
Hello interval is 5 sec
Next xmit serial <none>
Un/reliable mcasts: 0/0 Un/reliable ucasts: 0/0
Mcast exceptions: 0 CR packets: 0 ACKs suppressed: 0
Retransmissions sent: 0 Out-of-sequence rcvd: 0
Authentication mode is not set

The following sample output from the `show ipv6 eigrp interface detail` command displays detailed information about a specific interface on which the `no ipv6 next-hop self` command is configured with the `no-ecmp-mode` option:

```
DeviceDevice# show ipv6 eigrp interfaces detail tunnel 0

EIGRP-IPv6 Interfaces for AS(1)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Un/Reliable</th>
<th>Un/Reliable</th>
<th>SRTT</th>
<th>Un/Reliable</th>
<th>Flow Timer</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tu0/0</td>
<td>2</td>
<td>0/0</td>
<td>0/0</td>
<td>29</td>
<td>0/0</td>
<td>136</td>
<td>0</td>
</tr>
</tbody>
</table>

Hello-interval is 5, Hold-time is 15
Split-horizon is disabled
Next xmit serial <none>
Packetized sent/expedited: 48/1
Hello's sent/expedited: 13119/49
Un/reliable mcasts: 0/20 Un/reliable ucasts: 31/398
Mcast exceptions: 5 CR packets: 5 ACKs suppressed: 1
Retransmissions sent: 355 Out-of-sequence rcvd: 6
Next-hop-self disabled, next-hop info forwarded, **ECMP mode Enabled**
Topology-ids on interface - 0
Authentication mode is not set
```

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

**Table 27: show ipv6 eigrp interfaces Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface over which EIGRP is configured.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of directly connected EIGRP neighbors.</td>
</tr>
<tr>
<td>Xmit Queue Un/Reliable</td>
<td>Number of packets remaining in the Unreliable and Reliable transmit queues.</td>
</tr>
<tr>
<td>Mean SRTT</td>
<td>Mean smooth round-trip time (SRTT) interval (in seconds).</td>
</tr>
<tr>
<td>Pacing Time Un/Reliable</td>
<td>Pacing time (in seconds) used to determine when EIGRP packets (unreliable and reliable) should be sent out of the interface.</td>
</tr>
<tr>
<td>Multicast Flow Timer</td>
<td>Maximum number of seconds in which the device will send multicast EIGRP packets.</td>
</tr>
<tr>
<td>Pending Routes</td>
<td>Number of routes in the transmit queue waiting to be sent.</td>
</tr>
<tr>
<td>Hello interval is 5 sec</td>
<td>Length (in seconds) of the hello interval.</td>
</tr>
</tbody>
</table>
show ipv6 eigrp topology

To display Enhanced Interior Gateway Routing Protocol (EIGRP) IPv6 topology table entries, use the `show ipv6 eigrp topology` command in user EXEC or privileged EXEC mode.

```
show ipv6 eigrp topology [{as-number ipv6-address}] [{active | all-links | pending | summary | zero-successors}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>(Optional) Autonomous system number.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>(Optional) IPv6 address.</td>
</tr>
<tr>
<td>active</td>
<td>(Optional) Displays only active entries in the EIGRP topology table.</td>
</tr>
<tr>
<td>all-links</td>
<td>(Optional) Displays all entries in the EIGRP topology table (including nonfeasible-successor sources).</td>
</tr>
<tr>
<td>pending</td>
<td>(Optional) Displays all entries in the EIGRP topology table that are either waiting for an update from a neighbor or waiting to reply to a neighbor.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of the EIGRP topology table.</td>
</tr>
<tr>
<td>zero-successors</td>
<td>(Optional) Displays the available routes that have zero successors.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If this command is used without any keywords or arguments, only routes that are feasible successors are displayed. The `show ipv6 eigrp topology` command can be used to determine Diffusing Update Algorithm (DUAL) states and to debug possible DUAL problems.

**Examples**

The following is sample output from the `show ipv6 eigrp topology` command. The fields in the display are self-explanatory.

```
Device# show ipv6 eigrp topology
IPv6-EIGRP Topology Table for AS(1)/ID(2001:0DB8:10::/64)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:0DB8:3::/64, 1 successors, FD is 281600
via Connected, Ethernet1/0
```

The following sample output from the `show ipv6 eigrp topology prefix` command displays ECMP mode information when the `no ipv6 next-hop-self` command is configured without the `no-ecmp-mode` option in the EIGRP topology. The ECMP mode provides information about the path that is being
advertised. If there is more than one successor, the top most path will be advertised as the default path over all interfaces, and the message “ECMP Mode: Advertise by default” will be displayed in the output. If any path other than the default path is advertised, the message “ECMP Mode: Advertise out <Interface name>” will be displayed. The fields in the display are self-explanatory.

Device# show ipv6 eigrp topology 2001:DB8:10::1/128

EIGRP-IPv6 Topology Entry for AS(1)/ID(192.0.2.100) for 2001:DB8:10::1/128
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
Descriptor Blocks:
FE80::A8BB:CCFF:FE01:2E01 (Tunnel0), from FE80::A8BB:CCFF:FE01:2E01, Send flag is 0x0
Composite metric is (284160/281600), route is Internal
Vector metric:
Minimum bandwidth is 10000 Kbit
Total delay is 1100 microseconds
Reliability is 255/255
Load is ½55
Minimum MTU is 1400
Hop count is 1
Originating router is 10.10.1.1

ECMP Mode: Advertise by default

FE80::A8BB:CCFF:FE01:3E01 (Tunnel1), from FE80::A8BB:CCFF:FE01:3E01, Send flag is 0x0
Composite metric is (284160/281600), route is Internal
Vector metric:
Minimum bandwidth is 10000 Kbit
Total delay is 1100 microseconds
Reliability is 255/255
Load is ½55
Minimum MTU is 1400
Hop count is 1
Originating router is 10.10.2.2

ECMP Mode: Advertise out Tunnel1

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eigrp address-family topology</td>
<td>Displays entries in the EIGRP topology table.</td>
<td></td>
</tr>
</tbody>
</table>
show ipv6 eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv6 packets sent and received, use the `show ipv6 eigrp traffic` command in user EXEC or privileged EXEC mode.

**show ipv6 eigrp traffic** [as-number]

**Syntax Description**

- **as-number** (Optional) Autonomous system number.

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 eigrp traffic` command to provide information on packets received and sent.

**Examples**

The following is sample output from the `show ipv6 eigrp traffic` command:

```
Device# show ipv6 eigrp traffic
IPv6-EIGRP Traffic Statistics for process 9
    Hellos sent/received: 218/205
    Updates sent/received: 7/23
    Queries sent/received: 2/0
    Replies sent/received: 0/2
    Acks sent/received: 21/14
```

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

**Table 28: show ipv6 eigrp traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process 9</td>
<td>Autonomous system number specified in the <code>ipv6 router eigrp</code>command.</td>
</tr>
<tr>
<td>Hellos sent/received</td>
<td>Number of hello packets sent and received.</td>
</tr>
<tr>
<td>Updates sent/received</td>
<td>Number of update packets sent and received.</td>
</tr>
<tr>
<td>Queries sent/received</td>
<td>Number of query packets sent and received.</td>
</tr>
<tr>
<td>Replies sent/received</td>
<td>Number of reply packets sent and received.</td>
</tr>
<tr>
<td>Acks sent/received</td>
<td>Number of acknowledgment packets sent and received.</td>
</tr>
</tbody>
</table>
show ipv6 eigrp traffic

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ipv6 router eigrp</td>
<td>Configures the EIGRP for IPv6 routing process.</td>
</tr>
</tbody>
</table>
show ipv6 general-prefix

To display information on IPv6 general prefixes, use the **show ipv6 general-prefix** command in user EXEC or privileged EXEC mode.

**show ipv6 general-prefix**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the **show ipv6 general-prefix** command to view information on IPv6 general prefixes.

**Examples**

The following example shows an IPv6 general prefix called my-prefix, which has been defined based on a 6to4 interface. The general prefix is also being used to define an address on interface loopback42.

```
Device# show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4 2002:B0B:B0B::/48
   Loopback42 (Address command)
```

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

**Table 29: show ipv6 general-prefix Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Prefix</td>
<td>User-defined name of the IPv6 general prefix.</td>
</tr>
<tr>
<td>Acquired via</td>
<td>The general prefix has been defined based on a 6to4 interface. A general prefix can also be defined manually or acquired using DHCP for IPv6 prefix delegation.</td>
</tr>
<tr>
<td>2002:B0B:B0B::/48</td>
<td>The prefix value for this general prefix.</td>
</tr>
<tr>
<td>Loopback42 (Address command)</td>
<td>List of interfaces where this general prefix is used.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 general-prefix</td>
<td>Defines a general prefix for an IPv6 address manually.</td>
</tr>
</tbody>
</table>
show ipv6 interface

To display the usability status of interfaces configured for IPv6, use the **show ipv6 interface** command in user EXEC or privileged EXEC mode.

**Syntax**
```
show ipv6 interface [brief] [type number] [prefix]
```

**Syntax Description**
- **brief** (Optional) Displays a brief summary of IPv6 status and configuration for each interface.
- **type** (Optional) The interface type about which to display information.
- **number** (Optional) The interface number about which to display information.
- **prefix** (Optional) Prefix generated from a local IPv6 prefix pool.

**Command Default**
All IPv6 interfaces are displayed.

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The **show ipv6 interface** command provides output similar to the show ip interface command, except that it is IPv6-specific.

Use the **show ipv6 interface** command to validate the IPv6 status of an interface and its configured addresses. The show ipv6 interface command also displays the parameters that IPv6 is using for operation on this interface and any configured features.

If the interface’s hardware is usable, the interface is marked up. If the interface can provide two-way communication for IPv6, the line protocol is marked up.

If you specify an optional interface type and number, the command displays information only about that specific interface. For a specific interface, you can enter the prefix keyword to see the IPv6 neighbor discovery (ND) prefixes that are configured on the interface.

**Interface Information for a Specific Interface with IPv6 Configured**
The **show ipv6 interface** command displays information about the specified interface.

```
Device(config)# show ipv6 interface ethernet0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:6700
No Virtual link-local address(es):
Global unicast address(es):
  2001::1, subnet is 2001::/64 [DUP]
  2001::A8BB:CCFF:FE00:6700, subnet is 2001::/64 [EUI]
  2001:100::1, subnet is 2001:100::/64
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Joined group address(es):
FF02::1
FF02::2
FF02::1:FF00:1
FF02::1:FF00:6700

MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND advertised reachable time is 0 (unspecified)
ND advertised retransmit interval is 0 (unspecified)
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium

Hosts use stateless autoconfig for addresses.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet0/0 is up, line protocol is up</td>
<td>Indicates whether the interface hardware is active (whether line signal is present) and whether it has been taken down by an administrator. If the interface hardware is usable, the interface is marked &quot;up.&quot; For an interface to be usable, both the interface hardware and line protocol must be up.</td>
</tr>
<tr>
<td>line protocol is up, down (down is not shown in sample output)</td>
<td>Indicates whether the software processes that handle the line protocol consider the line usable (that is, whether keepalives are successful or IPv6 CP has been negotiated). If the interface can provide two-way communication, the line protocol is marked up. For an interface to be usable, both the interface hardware and line protocol must be up.</td>
</tr>
<tr>
<td>IPv6 is enabled, stalled, disabled (stalled and disabled are not shown in sample output)</td>
<td>Indicates that IPv6 is enabled, stalled, or disabled on the interface. If IPv6 is enabled, the interface is marked &quot;enabled.&quot; If duplicate address detection processing identified the link-local address of the interface as being a duplicate address, the processing of IPv6 packets is disabled on the interface and the interface is marked &quot;stalled.&quot; If IPv6 is not enabled, the interface is marked &quot;disabled.&quot;</td>
</tr>
<tr>
<td>link-local address</td>
<td>Displays the link-local address assigned to the interface.</td>
</tr>
<tr>
<td>Global unicast address(es):</td>
<td>Displays the global unicast addresses assigned to the interface.</td>
</tr>
<tr>
<td>Joined group address(es):</td>
<td>Indicates the multicast groups to which this interface belongs.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit of the interface.</td>
</tr>
<tr>
<td>ICMP error messages</td>
<td>Specifies the minimum interval (in milliseconds) between error messages sent on this interface.</td>
</tr>
<tr>
<td>ICMP redirects</td>
<td>The state of Internet Control Message Protocol (ICMP) IPv6 redirect messages on the interface (the sending of the messages is enabled or disabled).</td>
</tr>
</tbody>
</table>
The `show ipv6 interface` command displays information about attributes that may be associated with an IPv6 address assigned to the interface.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>Anycast. The address is an anycast address, as specified when configured using the <code>ipv6 address</code> command.</td>
</tr>
<tr>
<td>CAL</td>
<td>Calendar. The address is timed and has valid and preferred lifetimes.</td>
</tr>
<tr>
<td>DEP</td>
<td>Deprecated. The timed address is deprecated.</td>
</tr>
<tr>
<td>DUP</td>
<td>Duplicate. The address is a duplicate, as determined by duplicate address detection (DAD). To re-attempt DAD, the user must use the <code>shutdown</code> or <code>no shutdown</code> command on the interface.</td>
</tr>
<tr>
<td>EUI</td>
<td>EUI-64 based. The address was generated using EUI-64.</td>
</tr>
<tr>
<td>OFF</td>
<td>Offlink. The address is offlink.</td>
</tr>
</tbody>
</table>
**Attribute** | **Description**
--- | ---
OOD | Overly optimistic DAD. DAD will not be performed for this address. This attribute applies to virtual addresses.
PRE | Preferred. The timed address is preferred.
TEN | Tentative. The address is in a tentative state per DAD.
UNA | Unactivated. The virtual address is not active and is in a standby state.
VIRT | Virtual. The address is virtual and is managed by HSRP, VRRP, or GLBP.

**show ipv6 interface Command Using the brief Keyword**

The following is sample output from the `show ipv6 interface` command when entered with the `brief` keyword:

```
Device# show ipv6 interface brief
Ethernet0 is up, line protocol is up
  Ethernet0 [up/up] unassigned
  Ethernet1 [up/up] 2001:0DB8:1000:/29
  Ethernet2 [up/up] 2001:0DB8:2000:/29
  Ethernet3 [up/up] 2001:0DB8:3000:/29
  Ethernet4 [up/down] 2001:0DB8:4000:/29
  Ethernet5 [administratively down/down] 2001:123::210:7BFF:FEC2:ACD8

Interface Status IPv6 Address
Ethernet0 up 3FFE:C00:0:1:260:3EFF:FE11:6770
Ethernet1 up unassigned
Fddi0 up 3FFE:C00:0:2:260:3EFF:FE11:6772
Serial0 administratively down unassigned
Serial1 administratively down unassigned
Serial2 administratively down unassigned
Serial3 administratively down unassigned
Tunnel0 up unnumbered (Ethernet0)
Tunnel1 up 3FFE:700:20:1::12
```

**IPv6 Interface with ND Prefix Configured**

This sample output shows the characteristics of an interface that has generated a prefix from a local IPv6 prefix pool:

```
Device# show ipv6 interface Ethernet 0/0 prefix

interface Ethernet0/0
  ipv6 address 2001:0DB8::1/64
  ipv6 address 2001:0DB8::2/64
```
ipv6 nd prefix 2001:0DB8:2::/64
ipv6 nd prefix 2001:0DB8:3::/64 2592000 604800 off-link
end
.
.
IPv6 Prefix Advertisements Ethernet0/0
Codes: A - Address, P - Prefix-Advertisement, O - Pool
U - Per-user prefix, D - Default
N - Not advertised, C - Calendar
default [LA] Valid lifetime 2592000, preferred lifetime 604800
AD 2001:0DB8:1::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
APD 2001:0DB8:2::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
P 2001:0DB8:3::/64 [A] Valid lifetime 2592000, preferred lifetime 604800

The default prefix shows the parameters that are configured using the ipv6 nd prefix default command.

IPv6 Interface with DRP Configured

This sample output shows the state of the DRP preference value as advertised by this device through an interface:

Device# show ipv6 interface gigabitethernet 0/1
GigabitEthernet0/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::130
Description: Management network (dual stack)
Global unicast address(es):
  FEC0:240:104:1000::130, subnet is FEC0:240:104:1000::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::1:FF00:130
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Low
Hosts use stateless autoconfig for addresses.

IPv6 Interface with HSRP Configured

When HSRP IPv6 is first configured on an interface, the interface IPv6 link-local address is marked unactive (UNA) because it is no longer advertised, and the HSRP IPv6 virtual link-local address is added to the virtual link-local address list with the UNA and tentative DAD (TEN) attributes set. The interface is also programmed to listen for the HSRP IPv6 multicast address.

This sample output shows the status of UNA and TEN attributes, when HSRP IPv6 is configured on an interface:

Device# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
Virtual link-local address(es):
FE80::205:73FF:FEA0:1 [UNA/TEN]
Global unicast address(es):
  2001:2::2, subnet is 2001:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::66
  FF02::1:FF00:2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ND DAD is enabled, number of DAD attempts: 1

After the HSRP group becomes active, the UNA and TEN attributes are cleared, and the overly optimistic DAD (OOD) attribute is set. The solicited node multicast address for the HSRP virtual IPv6 address is also added to the interface.

This sample output shows the status of UNA, TEN and OOD attributes, when HSRP group is activated:

```
# show ipv6 interface ethernet 0/0
Ethernet0/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80:2::2 [UNA]
Virtual link-local address(es):
  FE80::205:73FF:FEA0:1 [OPT]
Global unicast address(es):
  2001:2::2, subnet is 2001:2::/64
Joined group address(es):
  FF02::1
  FF02::2
  FF02::66
  FF02::1:FF00:2
  FF02::1:FFA0:1
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
```

The table below describes additional significant fields shown in the displays for the `show ipv6 interface` command with HSRP configured.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 is enabled, link-local address is FE80::2::2 [UNA]</td>
<td>The interface IPv6 link-local address is marked UNA because it is no longer advertised.</td>
</tr>
<tr>
<td>FE80::205:73FF:FEA0:1 [UNA/TEN]</td>
<td>The virtual link-local address list with the UNA and TEN attributes set.</td>
</tr>
<tr>
<td>FF02::66</td>
<td>HSRP IPv6 multicast address.</td>
</tr>
<tr>
<td>FE80::205:73FF:FEA0:1 [OPT]</td>
<td>HSRP becomes active, and the HSRP virtual address marked OPT.</td>
</tr>
<tr>
<td>FF02::1:FFA0:1</td>
<td>HSRP solicited node multicast address.</td>
</tr>
</tbody>
</table>
IPv6 Interface with Minimum RA Interval Configured

When you enable Mobile IPv6 on an interface, you can configure a minimum interval between IPv6 router advertisement (RA) transmissions. The `show ipv6 interface` command output reports the minimum RA interval, when configured. If the minimum RA interval is not explicitly configured, then it is not displayed.

In the following example, the maximum RA interval is configured as 100 seconds, and the minimum RA interval is configured as 60 seconds on Ethernet interface 1/0:

```
Device(config-if)# ipv6 nd ra-interval 100 60
```

Subsequent use of the `show ipv6 interface` then displays the interval as follows:

```
Device(config)# show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
  FF02::1
  FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 60 to 100 seconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```

In the following example, the maximum RA interval is configured as 100 milliseconds (ms), and the minimum RA interval is configured as 60 ms on Ethernet interface 1/0:

```
Device(config)## show ipv6 interface ethernet 1/0
Ethernet1/0 is administratively down, line protocol is down
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:5A01 [TEN]
No Virtual link-local address(es):
No global unicast address is configured
Joined group address(es):
  FF02::1
  FF02::2
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachables are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 60 to 100 milliseconds
ND router advertisements live for 1800 seconds
ND advertised default router preference is Medium
Hosts use stateless autoconfig for addresses.
```
The table below describes additional significant fields shown in the displays for the show ipv6 interface command with minimum RA interval information configured.

**Table 32: show ipv6 interface Command with Minimum RA Interval Information Configuration Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ND router advertisements are sent every 60 to 100 seconds</td>
<td>ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 seconds, and the maximum value is 100 seconds.</td>
</tr>
<tr>
<td>ND router advertisements are sent every 60 to 100 milliseconds</td>
<td>ND RAs are sent at an interval randomly selected from a value between the minimum and maximum values. In this example, the minimum value is 60 ms, and the maximum value is 100 ms.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd prefix</td>
<td>Configures which IPv6 prefixes are included in IPv6 router advertisements.</td>
</tr>
<tr>
<td>ipv6 nd ra interval</td>
<td>Configures the interval between IPv6 RA transmissions on an interface.</td>
</tr>
<tr>
<td>show ip interface</td>
<td>Displays the usability status of interfaces configured for IP.</td>
</tr>
</tbody>
</table>
show ipv6 mfib

To display the forwarding entries and interfaces in the IPv6 Multicast Forwarding Information Base (MFIB), use the `show ipv6 mfib` command in user EXEC or privileged EXEC mode.

```
show ipv6 mfib [vrf vrf-name] [all | linkscope | verbose group-address-name | ipv6-prefix / prefix-length source-address-name | interface | status | summary]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Displays all forwarding entries and interfaces in the IPv6 MFIB.</td>
</tr>
<tr>
<td>linkscope</td>
<td>(Optional) Displays the link-local groups.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>(Optional) The IPv6 network assigned to the interface. The default IPv6 prefix is 128. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>/ prefix-length</td>
<td>(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td>group-address-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>source-address-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Interface settings and status.</td>
</tr>
<tr>
<td>status</td>
<td>(Optional) General settings and status.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 mfib` command to display MFIB entries; and forwarding interfaces, and their traffic statistics. This command can be enabled on virtual IP (VIP) if the router is operating in distributed mode.

A forwarding entry in the MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding...
behavior for packets received or forwarded on specific interfaces. The table below describes the MFIB forwarding entries and interface flags.

**Table 33: MFIB Entries and Interface Flags**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Forward--Data is forwarded out of this interface.</td>
</tr>
<tr>
<td>A</td>
<td>Accept--Data received on this interface is accepted for forwarding.</td>
</tr>
<tr>
<td>IC</td>
<td>Internal copy--Deliver to the router a copy of the packets received or forwarded on this interface.</td>
</tr>
<tr>
<td>NS</td>
<td>Negate signal--Reverse the default entry signaling behavior for packets received on this interface.</td>
</tr>
<tr>
<td>DP</td>
<td>Do not preserve--When signaling the reception of a packet on this interface, do not preserve a copy of it (discard it instead).</td>
</tr>
<tr>
<td>SP</td>
<td>Signal present--The reception of a packet on this interface was just signaled.</td>
</tr>
<tr>
<td>S</td>
<td>Signal--By default, signal the reception of packets matching this entry.</td>
</tr>
<tr>
<td>C</td>
<td>Perform directly connected check for packets matching this entry. Signal the reception if packets were originated by a directly connected source.</td>
</tr>
</tbody>
</table>

**Examples**

The following example displays the forwarding entries and interfaces in the MFIB. The router is configured for fast switching, and it has a receiver joined to FF05::1 on Ethernet1/1 and a source (2001::1:1:20) sending on Ethernet1/2:

```
Device# show ipv6 mfib
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
              IC - Internal Copy, NP - Not platform switched
              SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FF00::/8) Flags: C
   Forwarding: 0/0/0/0, Other: 0/0/0/0
   Tunnel0 Flags: NS
(*,FF00::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0/0
(*,FF05::1) Flags: C
   Forwarding: 2/0/100/0, Other: 0/0/0/0
   Tunnel0 Flags: A NS
   Ethernet1/1 Flags: F NS
   Pkts: 3/2
(2001::1:1:200,FF05::1) Flags:
   Forwarding: 5/0/100/0, Other: 0/0/0/0
   Ethernet1/2 Flags: A
   Ethernet1/1 Flags: F NS
   Pkts: 3/2
(*,FF10::/15) Flags: D
   Forwarding: 0/0/0/0, Other: 0/0/0/0
```

The table below describes the significant fields shown in the display.
Table 34: `show ipv6 mfib` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry Flags</td>
<td>Information about the entry.</td>
</tr>
<tr>
<td>Forwarding Counts</td>
<td>Statistics on the packets that are received from and forwarded to at least one interface.</td>
</tr>
<tr>
<td>Pkt Count/</td>
<td>Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.</td>
</tr>
<tr>
<td>Pkts per second/</td>
<td>Number of packets received and forwarded per second.</td>
</tr>
<tr>
<td>Avg Pkt Size/</td>
<td>Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.</td>
</tr>
<tr>
<td>Kbits per second</td>
<td>Bytes per second divided by packets per second divided by 1000.</td>
</tr>
<tr>
<td>Other counts:</td>
<td>Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.</td>
</tr>
<tr>
<td>Interface Flags:</td>
<td>Information about the interface.</td>
</tr>
<tr>
<td>Interface Counts:</td>
<td>Interface statistics.</td>
</tr>
</tbody>
</table>

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03:1::1 specified:

```
Device# show ipv6 mfib FF03:1::1
IP Multicast Forwarding Information Base
Entry Flags:C - Directly Connected, S - Signal, IA - Inherit A flag,
AR - Activity Required, D - Drop
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:Total/RFF failed/Other drops
Interface Flags:A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts:FS Pkt Count/FS Pkt Count
,FF03:1::1) Flags:C
Forwarding:0/0/0/0, Other:0/0/0
Tunnel1 Flags:A NS
GigabitEthernet5/0.25 Flags:F NS
Pkts:0/0
GigabitEthernet5/0.24 Flags:F NS
Pkts:0/0
(5002:1::2,FF03:1::1) Flags:
Forwarding:71505/0/50/0, Other:42/0/42
GigabitEthernet5/0 Flags:A
GigabitEthernet5/0.19 Flags:F NS
Pkts:239/24
GigabitEthernet5/0.20 Flags:F NS
Pkts:239/24
GigabitEthernet5/0.21 Flags:F NS
Pkts:238/24
```
The following examples show forwarding entries and interfaces in the MFIB, with a group address of FF03::1 and a source address of 5002::1::2 specified:

Device# show ipv6 mfib FF03::1 5002::1::2

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FF03::1 and a default prefix of 128:

Device# show ipv6 mfib FF03::1/128

The following example shows forwarding entries and interfaces in the MFIB, with a group address of FFE0:: and a prefix of 15:

Device# show ipv6 mfib FFE0::/15
IP Multicast Forwarding Information Base

Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,FFE0::/15) Flags: D
Forwarding: 0/0/0/0, Other: 0/0/0

The following example shows output of the `show ipv6 mfib` command used with the `verbose` keyword. It shows forwarding entries and interfaces in the MFIB and additional information such as the MAC encapsulation header and platform-specific information.

Device# show ipv6 mfib ff33::1:1 verbose
IP Multicast Forwarding Information Base
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag, AR - Activity Required, K - Keepalive
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Platform per slot HW-Forwarding Counts: Pkt Count/Byte Count
Platform flags: HF - Forwarding entry, HB - Bridge entry, HD - NonRPF Drop entry, NP - Not platform switchable, RPL - RPF-ltl linkage,
MG - Metset change, ERR - S/w Error Flag, RTY - In RetryQ,
LP - L3 pending, MP - Met pending, AP - ACL pending
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
IC - Internal Copy, NP - Not platform switched
SP - Signal Present
Interface Counts: Distributed FS Pkt Count/FS Pkt Count/PS Pkt Count
(10::2,FF33::1:1) Flags: K
RP Forwarding: 0/0/0/0, Other: 0/0/0
LC Forwarding: 0/0/0/0, Other: 0/0/0
HW Forward: 0/0/0/0, Other: NA/NA/NA
Slot 6: HW Forwarding: 0/0, Platform Flags: HF RPL
Slot 1: HW Forwarding: 0/0, Platform Flags: HF RPL
Vlan10 Flags: A
Vlan30 Flags: F NS
Pkts: 0/0/0 MAC: 33330001000100D0FFE180086DD

The table below describes the fields shown in the display.

**Table 35: show ipv6 mfib verbose Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform flags</td>
<td>Information about the platform.</td>
</tr>
<tr>
<td>Platform per slot HW-Forwarding Counts</td>
<td>Total number of packets per bytes forwarded.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mfib active</td>
<td>Displays the rate at which active sources are sending to multicast groups.</td>
</tr>
<tr>
<td>show ipv6 mfib count</td>
<td>Displays summary traffic statistics from the MFIB about the group and source.</td>
</tr>
<tr>
<td>show ipv6 mfib interface</td>
<td>Displays information about IPv6 multicast-enabled interfaces and their forwarding status.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show ipv6 mfib status</code></td>
<td>Displays the general MFIB configuration and operational status.</td>
</tr>
<tr>
<td><code>show ipv6 mfib summary</code></td>
<td>Displays summary information about the number of IPv6 MFIB entries (including link-local groups) and interfaces.</td>
</tr>
</tbody>
</table>
show ipv6 mld groups

To display the multicast groups that are directly connected to the router and that were learned through Multicast Listener Discovery (MLD), use the `show ipv6 mld groups` command in user EXEC or privileged EXEC mode.

`show ipv6 mld [vrf vrf-name] groups [link-local] [[group-name|group-address]] [interface-type interface-number] [detail | explicit]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>link-local</td>
<td>(Optional) Displays the link-local groups.</td>
</tr>
<tr>
<td>group-name</td>
<td>group-address</td>
</tr>
<tr>
<td>interface-type interface-number</td>
<td>(Optional) Interface type and number.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information about individual sources.</td>
</tr>
<tr>
<td>explicit</td>
<td>(Optional) Displays information about the hosts being explicitly tracked on each interface for each group.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you omit all optional arguments, the `show ipv6 mld groups` command displays by group address and interface type and number all directly connected multicast groups, including link-local groups (where the `link-local` keyword is not available) used.

**Examples**

The following is sample output from the `show ipv6 mld groups` command. It shows all of the groups joined by Fast Ethernet interface 2/1, including link-local groups used by network protocols.

```
Device# show ipv6 mld groups FastEthernet 2/1
MLD Connected Group Membership
Group Address   Interface       Uptime   Expires
FF02::2         FastEthernet2/1  3d18h     never
FF02::D         FastEthernet2/1  3d18h     never
FF02::16        FastEthernet2/1  3d18h     never
FF02::1:FF00:1   FastEthernet2/1  3d18h 00:00:27
FF02::1:FF00:79  FastEthernet2/1  3d18h     never
FF02::1:FF23:83C2 FastEthernet2/1  3d18h 00:00:22
FF02::1:FFAF:2C39 FastEthernet2/1  3d18h     never
FF06:7777::1     FastEthernet2/1  3d18h 00:00:26
```

The following is sample output from the `show ipv6 mld groups` command using the `detail` keyword:
The following is sample output from the `show ipv6 mld groups` command using the `explicit` keyword:

```
Device# show ipv6 mld groups explicit
Ethernet1/0, FF05::1
    Up:00:43:11 EXCLUDE(0/1) Exp:00:03:17
    Host Address            Uptime   Expires  Fwd Flags
    FE80::A8BB:CCFF:FE00:800 00:43:11 00:03:17
    Mode:EXCLUDE
Ethernet1/0, FF05::6
    Up:00:42:22 INCLUDE(1/0) Exp:not used
    Host Address            Uptime   Expires  Fwd Flags
    FE80::A8BB:CCFF:FE00:800 00:42:22 00:03:17
    Mode:INCLUDE
300::1
300::2
300::3
Ethernet1/0 - Interface
ff05::1 - Group address
Up:Uptime for the group
EXCLUDE/INCLUDE - The mode the group is in on the router.
(0/1) (1/0) - (Number of hosts in INCLUDE mode/Number of hosts in EXCLUDE mode)
Exp:Expiry time for the group.
FE80::A8BB:CCFF:FE00:800 - Host ipv6 address.
00:43:11 - Uptime for the host.
00:03:17 - Expiry time for the host
Mode:INCLUDE/EXCLUDE - Mode the Host is operating in.
300::1, 300::2, 300::3 - Sources that the host has joined in the above specified mode.
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Address of the multicast group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the group is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>How long (in hours, minutes, and seconds) this multicast group has been known.</td>
</tr>
<tr>
<td>Expires</td>
<td>How long (in hours, minutes, and seconds) until the entry is removed from the MLD groups table.</td>
</tr>
<tr>
<td></td>
<td>The expiration timer shows &quot;never&quot; if the router itself has joined the group, and the expiration timer shows &quot;not used&quot; when the router mode of the group is INCLUDE. In this situation, the expiration timers on the source entries are used.</td>
</tr>
<tr>
<td>Last reporter</td>
<td>Last host to report being a member of the multicast group.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld query-interval</td>
<td>Configures the frequency at which the Cisco IOS software sends MLD host-query messages.</td>
</tr>
</tbody>
</table>
show ipv6 mld interface

To display multicast-related information about an interface, use the `show ipv6 mld interface` command in user EXEC or privileged EXEC mode.

```
show ipv6 mld [vrf vrf-name] interface [type number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>type number</td>
<td>(Optional) Interface type and number.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you omit the optional `type` and `number` arguments, the `show ipv6 mld interface` command displays information about all interfaces.

**Examples**

The following is sample output from the `show ipv6 mld interface` command for Ethernet interface 2/1/1:

```
Device# show ipv6 mld interface Ethernet 2/1/1
Global State Limit : 2 active out of 2 max
Loopback0 is administratively down, line protocol is down
   Internet address is ::/0
   .
   .
Ethernet2/1/1 is up, line protocol is up
   Internet address is FE80::260:3EFF:FE86:5649/10
   MLD is enabled on interface
   Current MLD version is 2
   MLD query interval is 125 seconds
   MLD querier timeout is 255 seconds
   MLD max query response time is 10 seconds
   Last member query response interval is 1 seconds
   Interface State Limit : 2 active out of 3 max
   State Limit permit access list:
   MLD activity: 83 joins, 63 leaves
   MLD querying router is FE80::260:3EFF:FE86:5649 (this system)
```

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

**Table 37: show ipv6 mld interface Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global State Limit: 2 active out of 2 max</td>
<td>Two globally configured MLD states are active.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ethernet2/1/1 is up, line protocol is up</td>
<td>Interface type, number, and status.</td>
</tr>
<tr>
<td>Internet address is...</td>
<td>Internet address of the interface and subnet mask being applied to the interface.</td>
</tr>
<tr>
<td>MLD is enabled in interface</td>
<td>Indicates whether Multicast Listener Discovery (MLD) has been enabled on the interface with the <code>ipv6 multicast-routing</code> command.</td>
</tr>
<tr>
<td>Current MLD version is 2</td>
<td>The current MLD version.</td>
</tr>
<tr>
<td>MLD query interval is 125 seconds</td>
<td>Interval (in seconds) at which the Cisco IOS software sends MLD query messages, as specified with the <code>ipv6 mld query-interval</code> command.</td>
</tr>
<tr>
<td>MLD querier timeout is 255 seconds</td>
<td>The length of time (in seconds) before the router takes over as the querier for the interface, as specified with the <code>ipv6 mld query-timeout</code> command.</td>
</tr>
<tr>
<td>MLD max query response time is 10 seconds</td>
<td>The length of time (in seconds) that hosts have to answer an MLD Query message before the router deletes their group, as specified with the <code>ipv6 mld query-max-response-time</code> command.</td>
</tr>
<tr>
<td>Last member query response interval is 1</td>
<td>Used to calculate the maximum response code inserted in group and source-specific query. Also used to tune the &quot;leave latency&quot; of the link. A lower value results in reduced time to detect the last member leaving the group.</td>
</tr>
<tr>
<td>Interface State Limit : 2 active out of 3</td>
<td>Two out of three configured interface states are active.</td>
</tr>
<tr>
<td>max</td>
<td></td>
</tr>
<tr>
<td>State Limit permit access list: change</td>
<td>Activity for the state permit access list.</td>
</tr>
<tr>
<td>MLD activity: 83 joins, 63 leaves</td>
<td>Number of groups joins and leaves that have been received.</td>
</tr>
<tr>
<td>MLD querying router is</td>
<td>IPv6 address of the querying router.</td>
</tr>
<tr>
<td>FE80::260:3EFF:FE86:5649 (this system)</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mld join-group</code></td>
<td>Configures MLD reporting for a specified group and source.</td>
</tr>
<tr>
<td><code>ipv6 mld query-interval</code></td>
<td>Configures the frequency at which the Cisco IOS software sends MLD host-query messages.</td>
</tr>
</tbody>
</table>
show ipv6 mld snooping

Use the `show ipv6 mld snooping` command in EXEC mode to display IP version 6 (IPv6) Multicast Listener Discovery (MLD) snooping configuration of the switch or the VLAN.

`show ipv6 mld snooping [vlan vlan-id]`

**Syntax Description**
- `vlan vlan-id` (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094.

**Command Modes**
- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display MLD snooping configuration for the switch or for a specific VLAN.

VLAN numbers 1002 through 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in MLD snooping.

To configure the dual IPv4 and IPv6 template, enter the `sdm prefer dual-ipv4-and-ipv6` global configuration command and reload the switch.

**Examples**

This is an example of output from the `show ipv6 mld snooping vlan` command. It shows snooping characteristics for a specific VLAN.

```
Device# show ipv6 mld snooping vlan 100
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
Vlan 100:
--------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000
```

This is an example of output from the `show ipv6 mld snooping` command. It displays snooping characteristics for all VLANs on the switch.
Device# show ipv6 mld snooping
Global MLD Snooping configuration:
-------------------------------------------
MLD snooping : Enabled
MLDv2 snooping (minimal) : Enabled
Listener message suppression : Enabled
TCN solicit query : Disabled
TCN flood query count : 2
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Vlan 1:
-------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 1
Last listener query count : 2
Last listener query interval : 1000

<output truncated>

Vlan 951:
-------
MLD snooping : Disabled
MLDv1 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmrp
Robustness variable : 3
Last listener query count : 2
Last listener query interval : 1000

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mld snooping</td>
<td>Enables and configures MLD snooping on the switch or on a VLAN.</td>
</tr>
<tr>
<td>sdm prefer</td>
<td>Configures an SDM template to optimize system resources based on how the switch is being used.</td>
</tr>
</tbody>
</table>
show ipv6 mld ssm-map

To display Source Specific Multicast (SSM) mapping information, use the `show ipv6 mld ssm-map static` command in user EXEC or privileged EXEC mode.

```
show ipv6 mld [vrf vrf-name] ssm-map [source-address]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) Source address associated with an MLD membership for a group identified by the access list.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the optional `source-address` argument is not used, all SSM mapping information is displayed.

**Examples**

The following example shows all SSM mappings for the router:

```
Device# show ipv6 mld ssm-map
SSM Mapping : Enabled
DNS Lookup : Enabled
```

The following examples show SSM mapping for the source address 2001:0DB8::1:

```
Device# show ipv6 mld ssm-map 2001:0DB8::1
Group address : 2001:0DB8::1
Group mode ssm : TRUE
Database : STATIC
Source list : 2001:0DB8::2
2001:0DB8::3
Router# show ipv6 mld ssm-map 2001:0DB8::2
Group address : 2001:0DB8::2
Group mode ssm : TRUE
Database : DNS
Source list : 2001:0DB8::3
2001:0DB8::1
```

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

**Table 38: show ipv6 mld ssm-map Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSM Mapping</td>
<td>The SSM mapping feature is enabled.</td>
</tr>
</tbody>
</table>
The DNS lookup feature is automatically enabled when the SSM mapping feature is enabled.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Lookup</td>
<td>The DNS lookup feature is automatically enabled when the SSM mapping feature is enabled.</td>
</tr>
<tr>
<td>Group address</td>
<td>Group address identified by a specific access list.</td>
</tr>
<tr>
<td>Group mode ssm : TRUE</td>
<td>The identified group is functioning in SSM mode.</td>
</tr>
<tr>
<td>Database : STATIC</td>
<td>The router is configured to determine source addresses by checking static SSM mapping configurations.</td>
</tr>
<tr>
<td>Database : DNS</td>
<td>The router is configured to determine source addresses using DNS-based SSM mapping.</td>
</tr>
<tr>
<td>Source list</td>
<td>Source address associated with a group identified by the access list.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 mld ssm-map</code></td>
<td>Displays debug messages for SSM mapping.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map enable</code></td>
<td>Enables the SSM mapping feature for groups in the configured SSM range</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map query dns</code></td>
<td>Enables DNS-based SSM mapping.</td>
</tr>
<tr>
<td><code>ipv6 mld ssm-map static</code></td>
<td>Configures static SSM mappings.</td>
</tr>
</tbody>
</table>
show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counters, use the `show ipv6 mld traffic` command in user EXEC or privileged EXEC mode.

```
show ipv6 mld [vrf vrf-name] traffic
```

**Syntax Description**

| vrf  | vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) configuration. |

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 mld traffic` command to check if the expected number of MLD protocol messages have been received and sent.

**Examples**

The following example displays the MLD protocol messages received and sent.

```
Device# show ipv6 mld traffic

MLD Traffic Counters
Elapsed time since counters cleared:00:00:21

Received  Sent
Valid MLD Packets  3       1
Queries            1       0
Reports            2       1
Leaves             0       0
Mtrace packets     0       0

Errors:
Malformed Packets  0
Bad Checksums      0
Martian source     0
Packets Received on MLD-disabled Interface 0
```

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

**Table 39: show ipv6 mld traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since</td>
<td>Indicates the amount of time (in hours, minutes, and seconds) since the</td>
</tr>
<tr>
<td>counters cleared</td>
<td>counters cleared.</td>
</tr>
<tr>
<td>Valid MLD packets</td>
<td>Number of valid MLD packets received and sent.</td>
</tr>
<tr>
<td>Queries</td>
<td>Number of valid queries received and sent.</td>
</tr>
</tbody>
</table>
### Field | Description
---|---
Reports | Number of valid reports received and sent.
Leaves | Number of valid leaves received and sent.
Mtrace packets | Number of multicast trace packets received and sent.
Errors | Types of errors and the number of errors that have occurred.
**show ipv6 mrib client**

To display information about the clients of the Multicast Routing Information Base (MRIB), use the `show ipv6 mrib client` command in user EXEC or privileged EXEC mode.

```
show ipv6 mrib [vrf vrf-name] client [filter] [name {client-name | client-name : client-id}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>filter</td>
<td>(Optional) Displays information about MRIB flags that each client owns and that each client is interested in.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) The name of a multicast routing protocol that acts as a client of MRIB, such as Multicast Listener Discovery (MLD) and Protocol Independent Multicast (PIM).</td>
</tr>
<tr>
<td>client-name : client-id</td>
<td>The name and ID of a multicast routing protocol that acts as a client of MRIB, such as MLD and PIM. The colon is required.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `filter` keyword to display information about the MRIB flags each client owns and the flags in which each client is interested.

**Examples**

The following is sample output from the `show ipv6 mrib client` command:

```
Device# show ipv6 mrib client
IP MRIB client-connections
igmp:145 (connection id 0)
pim:146 (connection id 1)
mfib ipv6:3 (connection id 2)
slot 3 mfib ipv6 rp agent:16 (connection id 3)
slot 1 mfib ipv6 rp agent:16 (connection id 4)
slot 0 mfib ipv6 rp agent:16 (connection id 5)
slot 4 mfib ipv6 rp agent:16 (connection id 6)
slot 2 mfib ipv6 rp agent:16 (connection id 7)
```

The table below describes the significant fields shown in the display.
### Table 40: show ipv6 mrib client Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp:145 (connection id 0) pim:146 (connection id 1) mfib ipv6:3 (connection id 2) mfib ipv6 rp agent:16 (connection id 3)</td>
<td>Client ID (client name:process ID)</td>
</tr>
</tbody>
</table>
show ipv6 mrib route

To display Multicast Routing Information Base (MRIB) route information, use the **show ipv6 mrib route** command in user EXEC or privileged EXEC mode.

```
show ipv6 mrib [vrf vrf-name] route [{link-local | summary | [{source-address source-name | *}] [groupname-or-address [prefix-length]]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>link-local</td>
<td>(Optional) Displays the link-local groups.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays the number of MRIB entries (including link-local groups) and interfaces present in the MRIB table.</td>
</tr>
<tr>
<td>source address-or-name</td>
<td>(Optional) IPv6 address or name of the source.</td>
</tr>
<tr>
<td>*</td>
<td>(Optional) Displays all MRIB route information.</td>
</tr>
<tr>
<td>groupname-or-address</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>prefix-length</td>
<td>(Optional) IPv6 prefix length.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

All entries are created by various clients of the MRIB, such as Multicast Listener Discovery (MLD), Protocol Independent Multicast (PIM), and Multicast Forwarding Information Base (MFIB). The flags on each entry or interface serve as a communication mechanism between various clients of the MRIB. The entries reveal how PIM sends register messages for new sources and the action taken.

The **summary** keyword shows the count of all entries, including link-local entries.

The interface flags are described in the table below.

**Table 41: Description of Interface Flags**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>Forward--Data is forwarded out of this interface</td>
</tr>
<tr>
<td>A</td>
<td>Accept--Data received on this interface is accepted for forwarding</td>
</tr>
<tr>
<td>IC</td>
<td>Internal copy</td>
</tr>
<tr>
<td>NS</td>
<td>Negate signal</td>
</tr>
</tbody>
</table>
Special entries in the MRIB indicate exceptions from the normal behavior. For example, no signaling or notification is necessary for arriving data packets that match any of the special group ranges. The special group ranges are as follows:

- Undefined scope (FFX0::/16)
- Node local groups (FFX1::/16)
- Link-local groups (FFX2::/16)
- Source Specific Multicast (SSM) groups (FF3X::/32).

For all the remaining (usually sparse-mode) IPv6 multicast groups, a directly connected check is performed and the PIM notified if a directly connected source arrives. This procedure is how PIM sends register messages for new sources.

**Examples**

The following is sample output from the `show ipv6 mrib route` command using the `summary` keyword:

```
Device# show ipv6 mrib route summary
MRIB Route-DB Summary
  No. of (*,G) routes = 52
  No. of (S,G) routes = 0
  No. of Route x Interfaces (RxI) = 10
```

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

**Table 42: show ipv6 mrib route Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of (*, G) routes</td>
<td>Number of shared tree routes in the MRIB.</td>
</tr>
<tr>
<td>No. of (S, G) routes</td>
<td>Number of source tree routes in the MRIB.</td>
</tr>
<tr>
<td>No. of Route x Interfaces</td>
<td>Sum of all the interfaces on each MRIB route entry.</td>
</tr>
</tbody>
</table>
show ipv6 mroute

To display the information in the PIM topology table in a format similar to the show ip mroute command, use the show ipv6 mroute command in user EXEC or privileged EXEC mode.

```
show ipv6 mroute [vrf vrf-name] [[link-local] [[group-name | group-address
[{{source-address|source-name}]]]] [summary] [count]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional)</td>
</tr>
<tr>
<td>link-local</td>
<td>(Optional)</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional)</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional)</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional)</td>
</tr>
<tr>
<td>source-name</td>
<td>(Optional)</td>
</tr>
</tbody>
</table>

### Command Default

The `show ipv6 mroute` command displays all groups and sources.

### Command Modes

User EXEC (>

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The IPv6 multicast implementation does not have a separate mroute table. For this reason, the `show ipv6 mroute` command enables you to display the information in the PIM topology table in a format similar to the `show ip mroute` command.

If you omit all optional arguments and keywords, the `show ipv6 mroute` command displays all the entries in the PIM topology table (except link-local groups where the `link-local` keyword is available).

The Cisco IOS software populates the PIM topology table by creating (S,G) and (*,G) entries based on PIM protocol messages, MLD reports, and traffic. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through Reverse Path Forwarding [RPF]).

Use the `show ipv6 mroute` command to display the forwarding status of each IPv6 multicast route.

### Examples

The following is sample output from the `show ipv6 mroute` command:
Device# show ipv6 mroute ff07::1
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
   C - Connected, L - Local, I - Received Source Specific Host Report,
   P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
   J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, FF07::1), 00:04:45/00:02:47, RP 2001:0DB8:6::6, flags:S
Incoming interface: Tunnel15
Outgoing interface list:
   POS4/0, Forward, 00:04:45/00:02:47
(2001:0DB8:999::99, FF07::1), 00:02:06/00:01:23, flags:SFT
Incoming interface: POS1/0
RPF nbr: 2001:0DB8:999::99
Outgoing interface list:
   POS4/0, Forward, 00:02:06/00:03:27

The following is sample output from the `show ipv6 mroute` command with the `summary` keyword:

Device# show ipv6 mroute ff07::1 summary
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
   C - Connected, L - Local, I - Received Source Specific Host Report,
   P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
   J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, FF07::1), 00:04:55/00:02:36, RP 2001:0DB8:6::6, flags:S
(2001:0DB8:999::99, FF07::1), 00:02:17/00:01:12, flags:SFT

The following is sample output from the `show ipv6 mroute` command with the `count` keyword:

Device# show ipv6 mroute ff07::1 count
IP Multicast Statistics
71 routes, 24 groups, 0.04 average sources per group
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts: Total/RPF failed/Other drops (OIF-null, rate-limit etc)
Group: FF07::1
   RP-tree:
      RP Forwarding: 0/0/0/0, Other: 0/0/0/0
      LC Forwarding: 0/0/0/0, Other: 0/0/0/0
   Source: 2001:0DB8:999::99
      RP Forwarding: 0/0/0/0, Other: 0/0/0/0
      LC Forwarding: 0/0/0/0, Other: 0/0/0/0
   HW Forwd: 2000/0/92/0, Other: 0/0/0/0
   Tot. shown: Source count: 1, pkt count: 20000

The table below describes the significant fields shown in the display.
### Table 43: `show ipv6 mroute` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags:</td>
<td>Provides information about the entry.</td>
</tr>
<tr>
<td></td>
<td>• S--sparse. Entry is operating in sparse mode.</td>
</tr>
<tr>
<td></td>
<td>• s--SSM group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.</td>
</tr>
<tr>
<td></td>
<td>• C--connected. A member of the multicast group is present on the directly connected interface.</td>
</tr>
<tr>
<td></td>
<td>• L--local. The router itself is a member of the multicast group.</td>
</tr>
<tr>
<td></td>
<td>• I--received source specific host report. Indicates that an (S, G) entry was created by an (S, G) report. This flag is set only on the designated router (DR).</td>
</tr>
<tr>
<td></td>
<td>• P--pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source.</td>
</tr>
<tr>
<td></td>
<td>• R--RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This is typically prune state along the shared tree for a particular source.</td>
</tr>
<tr>
<td></td>
<td>• F--register flag. Indicates that the software is registering for a multicast source.</td>
</tr>
<tr>
<td></td>
<td>• T--SPT-bit set. Indicates that packets have been received on the shortest path source tree.</td>
</tr>
<tr>
<td></td>
<td>• J--join SPT. For (<em>, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold value set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. The default SPT-Threshold value of 0 kbps is used for the group, and the J - Join SPT flag is always set on (</em>, G) entries and is never cleared. The router immediately switches to the shortest path source tree when traffic from a new source is received</td>
</tr>
<tr>
<td>Timers:</td>
<td>&quot;Uptime&quot; indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table. &quot;Expires&quot; indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.</td>
</tr>
<tr>
<td>Uptime/Expires</td>
<td></td>
</tr>
<tr>
<td>Interface state:</td>
<td>Indicates the state of the incoming or outgoing interface.</td>
</tr>
<tr>
<td></td>
<td>• Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list.</td>
</tr>
<tr>
<td></td>
<td>• Next-Hop. &quot;Next-Hop&quot; specifies the IP address of the downstream neighbor.</td>
</tr>
<tr>
<td></td>
<td>• State/Mode. &quot;State&quot; indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists. &quot;Mode&quot; indicates that the interface is operating in sparse mode.</td>
</tr>
</tbody>
</table>
Entry in the IPv6 multicast routing table. The entry consists of the IPv6 address of the source router followed by the IPv6 address of the multicast group. An asterisk (*) in place of the source router indicates all sources.

Entries in the first format are referred to as \((*, G)\) or "star comma G" entries. Entries in the second format are referred to as \((S, G)\) or "S comma G" entries; \((*, G)\) entries are used to build \((S, G)\) entries.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>((*, FF07::1)) and ((2001:0DB8:999::99))</td>
<td>Entry in the IPv6 multicast routing table. The entry consists of the IPv6 address of the source router followed by the IPv6 address of the multicast group. An asterisk (<em>) in place of the source router indicates all sources. Entries in the first format are referred to as ((</em>, G)) or &quot;star comma G&quot; entries. Entries in the second format are referred to as ((S, G)) or &quot;S comma G&quot; entries.</td>
</tr>
<tr>
<td>RP</td>
<td>Address of the RP router.</td>
</tr>
<tr>
<td>flags:</td>
<td>Information set by the MRIB clients on this MRIB entry.</td>
</tr>
<tr>
<td>Incoming interface:</td>
<td>Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.</td>
</tr>
<tr>
<td>RPF nbr</td>
<td>IP address of the upstream router to the RP or source.</td>
</tr>
<tr>
<td>Outgoing interface list:</td>
<td>Interfaces through which packets will be forwarded. For ((S, G)) entries, this list will not include the interfaces inherited from the ((*, G)) entry.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 multicast-routing</td>
<td>Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.</td>
</tr>
<tr>
<td>show ipv6 mfib</td>
<td>Displays the forwarding entries and interfaces in the IPv6 MFIB.</td>
</tr>
</tbody>
</table>
show ipv6 mtu

To display maximum transmission unit (MTU) cache information for IPv6 interfaces, use the `show ipv6 mtu` command in user EXEC or privileged EXEC mode.

```
show ipv6 mtu [vrf vrfname]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Displays an IPv6 Virtual Private Network (VPN) routing/forwarding instance (VRF).</td>
</tr>
<tr>
<td>vrfname</td>
<td>(Optional) Name of the IPv6 VRF.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `vrf` keyword and `vrfname` argument allow you to view MTUs related to a specific VRF.

**Examples**

The following is sample output from the `show ipv6 mtu` command:

```
Device# show ipv6 mtu
MTU Since Destination Address
1400 00:04:21 5000:1::3
1280 00:04:50 FE80::203:A0FF:FED6:141D
```

The following is sample output from the `show ipv6 mtu` command using the `vrf` keyword and `vrfname` argument. This example provides information about the VRF named `vrfname1`:

```
Device# show ipv6 mtu vrf vrfname1
MTU Since Source Address Destination Address
1300 00:00:04 2001:0DB8:2 2001:0DB8:7
```

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

**Table 44: show ipv6 mtu Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTU</td>
<td>MTU, which was contained in the Internet Control Message Protocol (ICMP) packet-too-big message, used for the path to the destination address.</td>
</tr>
<tr>
<td>Since</td>
<td>Age of the entry since the ICMP packet-too-big message was received.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Address contained in the received ICMP packet-too-big message. Packets originating from this router to this address should be no bigger than the given MTU.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 mtu</td>
<td>Sets the MTU size of IPv6 packets sent on an interface.</td>
</tr>
</tbody>
</table>
show ipv6 nd destination

To display information about IPv6 host-mode destination cache entries, use the show ipv6 nd destination command in user EXEC or privileged EXEC mode.

`show ipv6 nd destination[vrf vrf-name][interface-type interface-number]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Specifies the Interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Specifies the Interface number.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the show ipv6 nd destination command to display information about IPv6 host-mode destination cache entries. If the vrf vrf-name keyword and argument pair is used, then only information about the specified VRF is displayed. If the interface-type and interface-number arguments are used, then only information about the specified interface is displayed.

**Examples**

```
Device# show ipv6 nd destination
IPv6 ND destination cache (table: default)
Code: R - Redirect
2001::1 [8]
   via FE80::A8BB:CCFF:FE00:5B00/Ethernet0/0
```

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

```
Table 45: show ipv6 nd destination Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code: R - Redirect</td>
<td>Destinations learned through redirect.</td>
</tr>
<tr>
<td>2001::1 [8]</td>
<td>The value displayed in brackets is the time, in seconds, since the destination cache entry was last used.</td>
</tr>
</tbody>
</table>
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd host mode strict</td>
<td>Enables the conformant, or strict, IPv6 host mode.</td>
</tr>
</tbody>
</table>
show ipv6 nd on-link prefix

To display information about on-link prefixes learned through router advertisements (RAs), use the `show ipv6 nd on-link prefix` command in user EXEC or privileged EXEC mode.

```
show ipv6 nd on-link prefix[vrf vrf-name][interface-type interface-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Specifies the Interface type.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Specifies the Interface number.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 nd on-link prefix` command to display information about on-link prefixes learned through RAs.

Prefixes learned from an RA may be inspected using the `show ipv6 nd on-link prefix` command. If the `vrf vrf-name` keyword and argument pair is used, then only information about the specified VRF is displayed. If the `interface-type` and `interface-number` arguments are used, then only information about the specified interface is displayed.

**Examples**

The following example displays information about on-link prefixes learned through RAs:

```
Device# show ipv6 nd on-link prefix
IPv6 ND on-link Prefix (table: default), 2 prefixes
Code: A - Autonomous Address Config
A 2001::/64 [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
2001:1::/64 [2591994/604794]
router FE80::A8BB:CCFF:FE00:5A00/Ethernet0/0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nd host mode strict</td>
<td>Enables the conformant, or strict, IPv6 host mode.</td>
</tr>
</tbody>
</table>
show ipv6 neighbors

To display IPv6 neighbor discovery (ND) cache information, use the `show ipv6 neighbors` command in user EXEC or privileged EXEC mode.

```
show ipv6 neighbors [{interface-type interface-number|ipv6-address|ipv6-hostname | statistics}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Specifies the type of the interface from which IPv6 neighbor information is to be displayed.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Specifies the number of the interface from which IPv6 neighbor information is to be displayed.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>(Optional) Specifies the IPv6 address of the neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>ipv6-hostname</td>
<td>(Optional) Specifies the IPv6 hostname of the remote networking device.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Displays ND cache statistics.</td>
</tr>
</tbody>
</table>

**Command Default**

All IPv6 ND cache entries are listed.

**Command Modes**

User EXEC (`>`)  
Privileged EXEC (`#`)  

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `interface-type` and `interface-number` arguments are not specified, cache information for all IPv6 neighbors is displayed. Specifying the `interface-type` and `interface-number` arguments displays only cache information about the specified interface.

Specifying the `statistics` keyword displays ND cache statistics.

The following is sample output from the `show ipv6 neighbors` command when entered with an interface type and number:

```
Device# show ipv6 neighbors ethernet 2
IPv6 Address Age Link-layer Addr State Interface
2000::0:10:4::2 0 0003.a0d6.141e REACH Ethernet2
FE80::203:AFF:FE6:141E 0 0003.a0d6.141e REACH Ethernet2
3001:1::45a - 0002.7d1a.9472 REACH Ethernet2
```

The following is sample output from the `show ipv6 neighbors` command when entered with an IPv6 address:
The table below describes the significant fields shown in the displays.

**Table 46: show ipv6 neighbors Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>IPv6 address of neighbor or interface.</td>
</tr>
<tr>
<td>Age</td>
<td>Time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.</td>
</tr>
<tr>
<td>Link-layer Addr</td>
<td>MAC address. If the address is unknown, a hyphen (-) is displayed.</td>
</tr>
<tr>
<td>State</td>
<td>The state of the neighbor cache entry. Following are the states for dynamic entries in the IPv6 neighbor discovery cache:</td>
</tr>
<tr>
<td></td>
<td>• INCMP (Incomplete)—Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.</td>
</tr>
<tr>
<td></td>
<td>• REACH (Reachable)—Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.</td>
</tr>
<tr>
<td></td>
<td>• STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.</td>
</tr>
<tr>
<td></td>
<td>• DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.</td>
</tr>
<tr>
<td></td>
<td>• PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.</td>
</tr>
<tr>
<td></td>
<td>• ?????—Unknown state.</td>
</tr>
</tbody>
</table>

Following are the possible states for static entries in the IPv6 neighbor discovery cache:

- INCMP (Incomplete)—The interface for this entry is down.
- REACH (Reachable)—The interface for this entry is up.

**Note**

Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface from which the address was reachable.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ipv6 neighbors` command with the `statistics` keyword:

```
Device# show ipv6 neighbor statistics

IPv6 ND Statistics
Entries 2, High-water 2, Gleaned 1, Scavenged 0
Entry States
  INCMP 0 REACH 0 STALE 2 GLEAN 0 DELAY 0 PROBE 0
Resolutions (INCMP)
  Requested 1, timeouts 0, resolved 1, failed 0
  In-progress 0, High-water 1, Throttled 0, Data discards 0
Resolutions (PROBE)
  Requested 3, timeouts 0, resolved 3, failed 0
```

The table below describes the significant fields shown in this display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entries</td>
<td>Total number of ND neighbor entries in the ND cache.</td>
</tr>
<tr>
<td>High-Water</td>
<td>Maximum amount (so far) of ND neighbor entries in ND cache.</td>
</tr>
<tr>
<td>Gleaned</td>
<td>Number of ND neighbor entries gleaned (that is, learned from a neighbor NA or other ND packet).</td>
</tr>
<tr>
<td>Scavenged</td>
<td>Number of stale ND neighbor entries that have timed out and been removed from the cache.</td>
</tr>
<tr>
<td>Entry States</td>
<td>Number of ND neighbor entries in each state.</td>
</tr>
<tr>
<td>Resolutions (INCMP)</td>
<td>Statistics for neighbor resolutions attempted in INCMP state (that is, resolutions prompted by a data packet). Details about the resolutions attempted in INCMP state are follows:</td>
</tr>
<tr>
<td></td>
<td>• Requested--Total number of resolutions requested.</td>
</tr>
<tr>
<td></td>
<td>• Timeouts--Number of timeouts during resolutions.</td>
</tr>
<tr>
<td></td>
<td>• Resolved--Number of successful resolutions.</td>
</tr>
<tr>
<td></td>
<td>• Failed--Number of unsuccessful resolutions.</td>
</tr>
<tr>
<td></td>
<td>• In-progress--Number of resolutions in progress.</td>
</tr>
<tr>
<td></td>
<td>• High-water--Maximum number (so far) of resolutions in progress.</td>
</tr>
<tr>
<td></td>
<td>• Throttled--Number of times resolution request was ignored due to maximum number of resolutions in progress limit.</td>
</tr>
<tr>
<td></td>
<td>• Data discards--Number of data packets discarded that are awaiting neighbor resolution.</td>
</tr>
</tbody>
</table>
Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet):

- Requested—Total number of resolutions requested.
- Timeouts—Number of timeouts during resolutions.
- Resolved—Number of successful resolutions.
- Failed—Number of unsuccessful resolutions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resolutions (PROBE)</td>
<td>Statistics for neighbor resolutions attempted in PROBE state (that is, re-resolutions of existing entries prompted by a data packet):</td>
</tr>
<tr>
<td></td>
<td>• Requested—Total number of resolutions requested.</td>
</tr>
<tr>
<td></td>
<td>• Timeouts—Number of timeouts during resolutions.</td>
</tr>
<tr>
<td></td>
<td>• Resolved—Number of successful resolutions.</td>
</tr>
<tr>
<td></td>
<td>• Failed—Number of unsuccessful resolutions.</td>
</tr>
</tbody>
</table>
**show ipv6 nhrp**

To display Next Hop Resolution Protocol (NHRP) mapping information, use the `show ipv6 nhrp` command in user EXEC or privileged EXEC mode.

```
show ipv6 nhrp [ { dynamic [ ipv6-address ] | incomplete | static } [ { address | interface } ] [ { brief | detail } ] ] [ purge ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dynamic</strong></td>
<td>(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.</td>
</tr>
<tr>
<td><strong>ipv6-address</strong></td>
<td>(Optional) The IPv6 address of the cache entry.</td>
</tr>
<tr>
<td><strong>incomplete</strong></td>
<td>(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.</td>
</tr>
<tr>
<td><strong>static</strong></td>
<td>(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the <code>ipv6 nhrp map</code> command. See the table below for types, number ranges, and descriptions.</td>
</tr>
<tr>
<td><strong>address</strong></td>
<td>(Optional) NHRP mapping entry for specified protocol addresses.</td>
</tr>
<tr>
<td><strong>interface</strong></td>
<td>(Optional) NHRP mapping entry for the specified interface. See the table below for types, number ranges, and descriptions.</td>
</tr>
<tr>
<td><strong>brief</strong></td>
<td>(Optional) Displays a short output of the NHRP mapping.</td>
</tr>
<tr>
<td><strong>detail</strong></td>
<td>(Optional) Displays detailed information about NHRP mapping.</td>
</tr>
<tr>
<td><strong>purge</strong></td>
<td>(Optional) Displays NHRP purge information.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (=>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 48: Valid Types, Number Ranges, and Interface Description

<table>
<thead>
<tr>
<th>Valid Types</th>
<th>Number Ranges</th>
<th>Interface Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>async</td>
<td>1</td>
<td>Async</td>
</tr>
<tr>
<td>atm</td>
<td>0 to 6</td>
<td>ATM</td>
</tr>
<tr>
<td>bvi</td>
<td>1 to 255</td>
<td>Bridge-Group Virtual Interface</td>
</tr>
<tr>
<td>cdma-ix</td>
<td>1</td>
<td>CDMA Ix</td>
</tr>
<tr>
<td>ctunnel</td>
<td>0 to 2147483647</td>
<td>C-Tunnel</td>
</tr>
<tr>
<td>dialer</td>
<td>0 to 20049</td>
<td>Dialer</td>
</tr>
<tr>
<td>ethernet</td>
<td>0 to 4294967295</td>
<td>Ethernet</td>
</tr>
<tr>
<td>fastethernet</td>
<td>0 to 6</td>
<td>FastEthernet IEEE 802.3</td>
</tr>
<tr>
<td>lex</td>
<td>0 to 2147483647</td>
<td>Lex</td>
</tr>
<tr>
<td>loopback</td>
<td>0 to 2147483647</td>
<td>Loopback</td>
</tr>
<tr>
<td>mfr</td>
<td>0 to 2147483647</td>
<td>Multilink Frame Relay bundle</td>
</tr>
<tr>
<td>multilink</td>
<td>0 to 2147483647</td>
<td>Multilink-group</td>
</tr>
<tr>
<td>null</td>
<td>0</td>
<td>Null</td>
</tr>
<tr>
<td>port-channel</td>
<td>1 to 64</td>
<td>Port channel</td>
</tr>
<tr>
<td>tunnel</td>
<td>0 to 2147483647</td>
<td>Tunnel</td>
</tr>
<tr>
<td>vif</td>
<td>1</td>
<td>PGM multicast host</td>
</tr>
<tr>
<td>virtual-ppp</td>
<td>0 to 2147483647</td>
<td>Virtual PPP</td>
</tr>
<tr>
<td>virtual-template</td>
<td>1 to 1000</td>
<td>Virtual template</td>
</tr>
<tr>
<td>virtual-tokenring</td>
<td>0 to 2147483647</td>
<td>Virtual Token Ring</td>
</tr>
<tr>
<td>xtagatm</td>
<td>0 to 2147483647</td>
<td>Extended tag ATM</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show ipv6 nhrp` command:

```
Device# show ipv6 nhrp
2001:0db8:13c4d:0015::1a2f:3d2c/48 via 2001:0db8:13c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

The table below describes the significant fields shown in the display.
Table 49: show ipv6 nhrp Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:0db8:3c4d:0015::1a2f:3d2c/48</td>
<td>Target network.</td>
</tr>
<tr>
<td>2001:0db8:3c4d:0015::1a2f:3d2c</td>
<td>Next hop to reach the target network.</td>
</tr>
<tr>
<td>Tunnel0</td>
<td>Interface through which the target network is reached.</td>
</tr>
<tr>
<td>created 6d05h</td>
<td>Length of time since the entry was created (dayshours).</td>
</tr>
<tr>
<td>never expire</td>
<td>Indicates that static entries never expire.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ipv6 nhrp` command using the `brief` keyword:

Device# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99

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

Table 50: show ipv6 nhrp brief Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48</td>
<td>Target network.</td>
</tr>
<tr>
<td>via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c</td>
<td>Next Hop to reach the target network.</td>
</tr>
<tr>
<td>Interface: Tunnel0</td>
<td>Interface through which the target network is reached.</td>
</tr>
</tbody>
</table>
| Type: static           | Type of tunnel. The types can be one of the following:
|                        | • dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. |
|                        | • static--NHRP mapping is configured statically. Entries configured by the `ipv6 nhrp map` command are marked static. |
|                        | • incomplete--The NBMA address is not known for the target network. |

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 nhrp map</td>
<td>Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.</td>
</tr>
</tbody>
</table>
show ipv6 ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the show ipv6 ospf command in user EXEC or privileged EXEC mode.

```
show ipv6 ospf [process-id] [area-id] [rate-limit]
```

**Syntax Description**
- **process-id** (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.
- **area-id** (Optional) Area ID. This argument displays information about a specified area only.
- **rate-limit** (Optional) Rate-limited link-state advertisements (LSAs). This keyword displays LSAs that are currently being rate limited, together with the remaining time to the next generation.

**Command Modes**
- User EXEC (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**show ipv6 ospf Output Example**

The following is sample output from the show ipv6 ospf command:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.10.10.1
  SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
  Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  Number of external LSA 0. Checksum Sum 0x000000
  Number of interfaces in this device is 1. 1 normal 0 stub 0 nssa
  Area BACKBONE(0)
    Number of interfaces in this area is 1
    MD5 Authentication, SPI 1000
    SPF algorithm executed 2 times
    Number of LSA 5. Checksum Sum 0x02A005
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

The table below describes the significant fields shown in the display.
Table 51: show ipv6 ospf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process &quot;ospfv3 1&quot;</td>
<td>Process ID and OSPF device ID.</td>
</tr>
<tr>
<td>with ID 10.10.10.1</td>
<td></td>
</tr>
<tr>
<td>LSA group pacing timer</td>
<td>Configured LSA group pacing timer (in seconds).</td>
</tr>
<tr>
<td>Interface flood pacing timer</td>
<td>Configured LSA flood pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Retransmission pacing timer</td>
<td>Configured LSA retransmission pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Number of areas</td>
<td>Number of areas in device, area addresses, and so on.</td>
</tr>
</tbody>
</table>

show ipv6 ospf With Area Encryption Example

The following sample output shows the `show ipv6 ospf` command with area encryption information:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.0.0.1
It is an area border device
SPF schedule delay 5 secs, Hold time between two SPF's 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of areas in this device is 2. 2 normal 0 stub 0 nssa
Reference bandwidth unit is 100 mbps
Area BACKBONE(0)
  Number of interfaces in this area is 2
  SPF algorithm executed 3 times
  Number of LSA 31. Checksum Sum 0x107493
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 20
  Flood list length 0
Area 1
  Number of interfaces in this area is 2
  NULL Encryption SHA-1 Auth, SPI 1001
  SPF algorithm executed 7 times
  Number of LSA 20. Checksum Sum 0x095E6A
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

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

Table 52: show ipv6 ospf with Area Encryption Information Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area 1</td>
<td>Subsequent fields describe area 1.</td>
</tr>
</tbody>
</table>
null Encryption SHA-1 Auth, SPI 1001

Displays the encryption algorithm (in this case, null, meaning no encryption algorithm is used), the authentication algorithm (SHA-1), and the security policy index (SPI) value (1001).

The following example displays the configuration values for SPF and LSA throttling timers:

```
Device# show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary device
Redistributing External Routes from,
  ospf 2
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPFs 10000 msecs
  Maximum wait time between two consecutive SPFs 10000 msecs
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
```

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

### Table 53: show ipv6 ospf with SPF and LSA Throttling Timer Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial SPF schedule delay</td>
<td>Delay time of SPF calculations.</td>
</tr>
<tr>
<td>Minimum hold time between two consecutive SPFs</td>
<td>Minimum hold time between consecutive SPF calculations.</td>
</tr>
<tr>
<td>Maximum wait time between two consecutive SPFs 10000 msecs</td>
<td>Maximum hold time between consecutive SPF calculations.</td>
</tr>
<tr>
<td>Minimum LSA interval 5 secs</td>
<td>Minimum time interval (in seconds) between link-state advertisements.</td>
</tr>
<tr>
<td>Minimum LSA arrival 1000 msecs</td>
<td>Maximum arrival time (in milliseconds) of link-state advertisements.</td>
</tr>
</tbody>
</table>

The following example shows information about LSAs that are currently being rate limited:

```
Device# show ipv6 ospf rate-limit
List of LSAs that are in rate limit Queue
  LSADID: 0.0.0.0 Type: 0x2001 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
  LSADID: 0.0.0.0 Type: 0x2009 Adv Rtr: 10.55.55.55 Due in: 00:00:00.500
```

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

### Table 54: show ipv6 ospf rate-limit Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSAID</td>
<td>Link-state ID of the LSA.</td>
</tr>
<tr>
<td>Type</td>
<td>Description of the LSA.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Adv Rtr</td>
<td>ID of the advertising device.</td>
</tr>
<tr>
<td>Due in:</td>
<td>Remaining time until the generation of the next event.</td>
</tr>
</tbody>
</table>
show ipv6 ospf border-routers

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the `show ipv6 ospf border-routers` command in user EXEC or privileged EXEC mode.

```
show ip ospf [process-id] border-routers
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ipv6 ospf border-routers` command:

```
Device# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

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

**Table 55: show ipv6 ospf border-routers Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>i - Intra-area route, I - Inter-area route</td>
<td>The type of this route.</td>
</tr>
<tr>
<td>172.16.4.4, 172.16.3.3</td>
<td>Router ID of the destination router.</td>
</tr>
<tr>
<td>[2], [1]</td>
<td>Metric used to reach the destination router.</td>
</tr>
<tr>
<td>FastEthernet0/0, POS4/0</td>
<td>The interface on which the IPv6 OSPF protocol is configured.</td>
</tr>
<tr>
<td>ABR</td>
<td>Area border router.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ASBR</td>
<td>Autonomous system boundary router.</td>
</tr>
<tr>
<td>Area 0, Area 1</td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>SPF 13, SPF 8, SPF 3</td>
<td>The internal number of the shortest path first (SPF) calculation that installs this route.</td>
</tr>
</tbody>
</table>
show ipv6 ospf event

To display detailed information about IPv6 Open Shortest Path First (OSPF) events, use the **show ipv6 ospf event** command in privileged EXEC mode.

```
show ipv6 ospf [process-id] event [{generic | interface | lsa | neighbor | reverse | rib | spf}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
<tr>
<td>generic</td>
<td>(Optional) Generic information regarding OSPF for IPv6 events.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Interface state change events, including old and new states.</td>
</tr>
<tr>
<td>lsa</td>
<td>(Optional) LSA arrival and LSA generation events.</td>
</tr>
<tr>
<td>neighbor</td>
<td>(Optional) Neighbor state change events, including old and new states.</td>
</tr>
<tr>
<td>reverse</td>
<td>(Optional) Keyword to allow the display of events in reverse-from the latest to the oldest or from oldest to the latest.</td>
</tr>
<tr>
<td>rib</td>
<td>(Optional) Routing Information Base (RIB) update, delete, and redistribution events.</td>
</tr>
<tr>
<td>spf</td>
<td>(Optional) Scheduling and SPF run events.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An OSPF event log is kept for every OSPF instance. If you enter no keywords with the **show ipv6 ospf event** command, all information in the OSPF event log is displayed. Use the keywords to filter specific information.

**Examples**

The following example shows scheduling and SPF run events, LSA arrival and LSA generation events, in order from the oldest events to the latest generated events:

```
Device# show ipv6 ospf event spf lsa reverse

OSPFv3 Router with ID (10.0.0.1) (Process ID 1)
1 *Sep 29 11:59:18.367: Rcv Changed Type-0x2009 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1, Seq# 80007699, Age 3600
3 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type P
4 *Sep 29 11:59:18.367: Rcv Changed Type-0x2001 LSA, LSID 10.0.0.0, Adv-Rtr 192.168.0.1, Seq# 80007699, Age 2
5 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.0.0.0, LSA type R
6 *Sep 29 11:59:18.367: Rcv Changed Type-0x2002 LSA, LSID 10.1.0.1, Adv-Rtr 192.168.0.1, Seq# 80007699, Age 3600
8 *Sep 29 11:59:18.367: Schedule SPF, Area 0, Change in LSID 10.1.0.1, LSA type N
```
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Router with ID (10.0.0.1) (Process ID 1)</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Rcv Changed Type-0x2009 LSA</td>
<td>Description of newly arrived LSA.</td>
</tr>
<tr>
<td>LSID</td>
<td>Link-state ID of the LSA.</td>
</tr>
<tr>
<td>Adv-Rtr</td>
<td>ID of the advertising router.</td>
</tr>
<tr>
<td>Seq#</td>
<td>Link state sequence number (detects old or duplicate link state advertisements).</td>
</tr>
<tr>
<td>Age</td>
<td>Link state age (in seconds).</td>
</tr>
<tr>
<td>Schedule SPF</td>
<td>Enables SPF to run.</td>
</tr>
<tr>
<td>Area</td>
<td>OSPF area ID.</td>
</tr>
<tr>
<td>Change in LSID</td>
<td>Changed link-state ID of the LSA.</td>
</tr>
<tr>
<td>LSA type</td>
<td>LSA type.</td>
</tr>
</tbody>
</table>
show ipv6 ospf event
show ipv6 ospf graceful-restart

To display Open Shortest Path First for IPv6 (OSPFv3) graceful restart information, use the `show ipv6 ospf graceful-restart` command in privileged EXEC mode.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `show ipv6 ospf graceful-restart` command to discover information about the OSPFv3 graceful restart feature.

Examples

The following example displays OSPFv3 graceful restart information:

```plaintext
Device# show ipv6 ospf graceful-restart
Routing Process "ospf 1"
    Graceful Restart enabled
        restart-interval limit: 120 sec, last restart 00:00:15 ago (took 36 secs)
        Graceful Restart helper support enabled
        Router status : Active
        Router is running in SSO mode
        OSPF restart state : NO_RESTART
        Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Process &quot;ospf 1&quot;</td>
<td>The OSPFv3 routing process ID.</td>
</tr>
<tr>
<td>Graceful Restart enabled</td>
<td>The graceful restart feature is enabled on this router.</td>
</tr>
<tr>
<td>restart-interval limit: 120 sec</td>
<td>The restart-interval limit.</td>
</tr>
<tr>
<td>last restart 00:00:15 ago (took 36 secs)</td>
<td>How long ago the last graceful restart occurred, and how long it took to occur.</td>
</tr>
<tr>
<td>Graceful Restart helper support enabled</td>
<td>Graceful restart helper mode is enabled. Because graceful restart mode is also enabled on this router, you can identify this router as being graceful-restart capable. A router that is graceful-restart-aware cannot be configured in graceful-restart mode.</td>
</tr>
</tbody>
</table>
**show ipv6 ospf graceful-restart**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router status : Active</td>
<td>This router is in active, as opposed to standby, mode.</td>
</tr>
<tr>
<td>Router is running in SSO mode</td>
<td>The router is in stateful switchover mode.</td>
</tr>
<tr>
<td>OSPF restart state : NO_RESTART</td>
<td>The current OSPFv3 restart state.</td>
</tr>
<tr>
<td>Router ID 10.1.1.1, checkpoint Router ID 10.0.0.0</td>
<td>The IPv6 addresses of the current router and the checkpoint router.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf interface</td>
<td>Displays OSPFv3-related interface information.</td>
</tr>
</tbody>
</table>
show ipv6 ospf interface

To display Open Shortest Path First (OSPF)-related interface information, use the `show ipv6 ospf interface` command in user EXEC or privileged mode.

```
show ipv6 ospf [process-id] [area-id] interface [type number] [brief]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
<tr>
<td>area-id</td>
<td>(Optional) Displays information about a specified area only.</td>
</tr>
<tr>
<td>type number</td>
<td>(Optional) Interface type and number.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the router.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

show ipv6 ospf interface Standard Output Example

The following is sample output from the `show ipv6 ospf interface` command:

```
Device# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 1/1/1, flood queue length 0
Next 0x0(0)/0x0(0)/0x0(0)
Last flood scan length is 12, maximum is 12
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
   Adjacent with neighbor 172.16.6.6 (Designated Router)
   Suppress hello for 0 neighbor(s)

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATM3/0</td>
<td>Status of the physical link and operational status of protocol.</td>
</tr>
<tr>
<td>Link Local Address</td>
<td>Interface IPv6 address.</td>
</tr>
<tr>
<td>Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3</td>
<td>The area ID, process ID, instance ID, and router ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>Network Type POINT_TO_POINT, Cost: 1</td>
<td>Network type and link-state cost.</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>Transmit delay, interface state, and router priority.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>Designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Backup Designated router</td>
<td>Backup designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Timer intervals configured</td>
<td>Configuration of timer intervals.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of seconds until the next hello packet is sent out this interface.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Count of network neighbors and list of adjacent neighbors.</td>
</tr>
</tbody>
</table>

**Cisco IOS Release 12.2(33)SRB Example**

The following is sample output of the `show ipv6 ospf interface` command when the `brief` keyword is entered.

```
Device# show ipv6 ospf interface brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>PID</th>
<th>Area</th>
<th>Intf ID</th>
<th>Cost</th>
<th>State</th>
<th>Nbrs</th>
<th>F/C</th>
</tr>
</thead>
<tbody>
<tr>
<td>VL0</td>
<td>6</td>
<td>0</td>
<td>21</td>
<td>65535</td>
<td>DOWN</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>Se3/0</td>
<td>6</td>
<td>0</td>
<td>14</td>
<td>64</td>
<td>P2P</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>Lo1</td>
<td>6</td>
<td>0</td>
<td>20</td>
<td>1</td>
<td>LOOP</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>Se2/0</td>
<td>6</td>
<td>6</td>
<td>10</td>
<td>62</td>
<td>P2P</td>
<td>0/0</td>
<td></td>
</tr>
<tr>
<td>Tu0</td>
<td>1000</td>
<td>0</td>
<td>19</td>
<td>11111</td>
<td>DOWN</td>
<td>0/0</td>
<td></td>
</tr>
</tbody>
</table>
```
OSPF with Authentication on the Interface Example

The following is sample output from the `show ipv6 ospf interface` command with authentication enabled on the interface:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication SPI 500, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address 2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:01
  Index 1/1/1, flood queue length 0
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Null Authentication Example

The following is sample output from the `show ipv6 ospf interface` command with null authentication configured on the interface:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  Authentication NULL
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address 2001:0DB1:A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)
```

OSPF with Authentication for the Area Example

The following is sample output from the `show ipv6 ospf interface` command with authentication configured for the area:

```
Device# show ipv6 ospf interface
```
Ethernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:6E00, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.10.10.1
  Network Type BROADCAST, Cost:10
  MD5 Authentication (Area) SPI 1000, secure socket state UP (errors:0)
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 10.11.11.1, local address 2001:0DB1:A8BB:CCFF:FE00:6F00
  Backup Designated router (ID) 10.10.10.1, local address FE80::A8BB:CCFF:FE00:6E00
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:03
  Index 1/1/1, flood queue length 0
  Last flood scan length is 1, maximum is 1
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.11.11.1 (Designated Router)
  Suppress hello for 0 neighbor(s)

OSPF with Dynamic Cost Example

The following display shows sample output from the `show ipv6 ospf interface` command when the OSPF cost dynamic is configured.

```
Device# show ipv6 ospf interface serial 2/0
Serial2/0 is up, line protocol is up
  Link Local Address 2001:0DB1:A8BB:CCFF:FE00:100, Interface ID 10
  Area 1, Process ID 1, Instance ID 0, Router ID 172.1.1.1
  Network Type POINT_TO_MULTIPOINT, Cost: 64 (dynamic), Cost Hysteresis: 200
  Cost Weights: Throughput 100, Resources 20, Latency 80, L2-factor 100
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
  Hello due in 00:00:19
  Index 1/2/3, flood queue length 0
  Last flood scan length is 0, maximum is 0
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

OSPF Graceful Restart Example

The following display shows sample output from the `show ipv6 ospf interface` command when the OSPF graceful restart feature is configured:

```
Device# show ipv6 ospf interface
Ethernet0/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:300, Interface ID 2
  Area 0, Process ID 1, Instance ID 0, Router ID 10.3.3.3
  Network Type POINT_TO_POINT, Cost: 10
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Graceful Restart p2p timeout in 00:00:19
  Hello due in 00:00:02
  Graceful Restart helper support enabled
  Index 1/1/1, flood queue length 0
  Last flood scan length is 1, maximum is 1
```
Example of an Enabled Protocol

The following display shows that the OSPF interface is enabled for Bidirectional Forwarding Detection (BFD):

```bash
Device# show ipv6 ospf interface
Serial10/0 is up, line protocol is up
  Link Local Address FE80::A8BB:CCFF:FE00:6500, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Neighbor Count is 1, Adjacent neighbor count is 1
  Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 ospf gracefull-restart</td>
<td>Displays OSPFv3 graceful restart information.</td>
<td></td>
</tr>
</tbody>
</table>
**show ipv6 ospf request-list**

To display a list of all link-state advertisements (LSAs) requested by a router, use the `show ipv6 ospf request-list` command in user EXEC or privileged EXEC mode.

```
show ipv6 ospf [process-id] [area-id] request-list [neighbor] [interface] [interface-neighbor]
```

**Syntax Description**

- `process-id` (Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the Open Shortest Path First (OSPF) routing process is enabled.
- `area-id` (Optional) Displays information only about a specified area.
- `neighbor` (Optional) Displays the list of all LSAs requested by the router from this neighbor.
- `interface` (Optional) Displays the list of all LSAs requested by the router from this interface.
- `interface-neighbor` (Optional) Displays the list of all LSAs requested by the router on this interface, from this neighbor.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The information displayed by the `show ipv6 ospf request-list` command is useful in debugging OSPF routing operations.

**Examples**

The following example shows information about the LSAs requested by the router:

```
Device# show ipv6 ospf request-list

OSPFV3 Router with ID (192.168.255.5) (Process ID 1)
Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

<table>
<thead>
<tr>
<th>Type</th>
<th>LS ID</th>
<th>ADV RTR</th>
<th>Seq NO</th>
<th>Age</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.3</td>
<td>0x800000C2</td>
<td>1</td>
<td>0x0014C5</td>
</tr>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.2</td>
<td>0x800000C8</td>
<td>0</td>
<td>0x00B8CA</td>
</tr>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>192.168.255.1</td>
<td>0x800000C5</td>
<td>1</td>
<td>0x008CD1</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.3</td>
<td>192.168.255.3</td>
<td>0x800000A9</td>
<td>774</td>
<td>0x0058C0</td>
</tr>
<tr>
<td>2</td>
<td>0.0.0.2</td>
<td>192.168.255.3</td>
<td>0x800000B7</td>
<td>1</td>
<td>0x003A63</td>
</tr>
</tbody>
</table>
```

The table below describes the significant fields shown in the display.
### Table 59: `show ipv6 ospf request-list` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Router with ID (192.168.255.5) (Process ID 1)</td>
<td>Identification of the router for which information is displayed.</td>
</tr>
<tr>
<td>Interface Ethernet0/0</td>
<td>Interface for which information is displayed.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of LSA.</td>
</tr>
<tr>
<td>LS ID</td>
<td>Link-state ID of the LSA.</td>
</tr>
<tr>
<td>ADV RTR</td>
<td>IP address of advertising router.</td>
</tr>
<tr>
<td>Seq NO</td>
<td>Sequence number of LSA.</td>
</tr>
<tr>
<td>Age</td>
<td>Age of LSA (in seconds).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum of LSA.</td>
</tr>
</tbody>
</table>
**show ipv6 ospf retransmission-list**

To display a list of all link-state advertisements (LSAs) waiting to be re-sent, use the `show ipv6 ospf retransmission-list` command in user EXEC or privileged EXEC mode.

```
show ipv6 ospf [process-id] [area-id] retransmission-list [neighbor] [interface] [interface-neighbor]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
<tr>
<td>area-id</td>
<td>(Optional) Displays information only about a specified area.</td>
</tr>
<tr>
<td>neighbor</td>
<td>(Optional) Displays the list of all LSAs waiting to be re-sent for this neighbor.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays the list of all LSAs waiting to be re-sent on this interface.</td>
</tr>
<tr>
<td>interface-neighbor</td>
<td>(Optional) Displays the list of all LSAs waiting to be re-sent on this interface, from this neighbor.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The information displayed by the `show ipv6 ospf retransmission-list` command is useful in debugging Open Shortest Path First (OSPF) routing operations.

**Examples**

The following is sample output from the `show ipv6 ospf retransmission-list` command:

```
Device# show ipv6 ospf retransmission-list

OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1
Type  LS ID  ADV RTR  Seq NO  Age Checksum
0x2001 0 192.168.255.2 0x80000222 1 0x00AE52
```

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

**Table 60: show ipv6 ospf retransmission-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Router with ID (192.168.255.2) (Process ID 1)</td>
<td>Identification of the router for which information is displayed.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Interface Ethernet0/0</td>
<td>Interface for which information is displayed.</td>
</tr>
<tr>
<td>Link state retransmission due in</td>
<td>Length of time before next link-state transmission.</td>
</tr>
<tr>
<td>Queue length</td>
<td>Number of elements in the retransmission queue.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of LSA.</td>
</tr>
<tr>
<td>LS ID</td>
<td>Link-state ID of the LSA.</td>
</tr>
<tr>
<td>ADV RTR</td>
<td>IP address of advertising router.</td>
</tr>
<tr>
<td>Seq NO</td>
<td>Sequence number of the LSA.</td>
</tr>
<tr>
<td>Age</td>
<td>Age of LSA (in seconds).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum of LSA.</td>
</tr>
</tbody>
</table>
show ipv6 ospf statistics

To display Open Shortest Path First for IPv6 (OSPFv6) shortest path first (SPF) calculation statistics, use the show ipv6 ospf statistics command in user EXEC or privileged EXEC mode.

show ipv6 ospf statistics [detail]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>(Optional) Displays statistics separately for each OSPF area and includes additional, more detailed statistics.</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The show ipv6 ospf statistics command provides important information about SPF calculations and the events that trigger them. This information can be meaningful for both OSPF network maintenance and troubleshooting. For example, entering the show ipv6 ospf statistics command is recommended as the first troubleshooting step for link-state advertisement (LSA) flapping.

Examples

The following example provides detailed statistics for each OSPFv6 area:

```
Device# show ipv6 ospf statistics detail
Area 0: SPF algorithm executed 3 times
SPF 1 executed 00:06:57 ago, SPF type Full
  SPF calculation time (in msec):
    SPF  Prefix D-Int Sum D-Sum Ext D-Ext Total
    0      0       0  0      0  0      0  0  0
  RIB manipulation time (in msec):
    RIB Update  RIB Delete
    0          0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X:0
  Change record R N SN SA L
  LSAs changed 1
  Changed LSAs. Recorded is Advertising Router, LSID and LS type: 10.2.2.2/0(R)
SPF 2 executed 00:06:47 ago, SPF type Full
  SPF calculation time (in msec):
    SPF  Prefix D-Int Sum D-Sum Ext D-Ext Total
    0      0       0  0      0  0      0  0  0
  RIB manipulation time (in msec):
    RIB Update  RIB Delete
    0          0
  LSIDs processed R:1 N:0 Prefix:1 SN:0 SA:0 X:0
  Change record R L P
  LSAs changed 4
  Changed LSAs. Recorded is Advertising Router, LSID and LS type: 10.2.2.2/2(L) 10.2.2.2/0(R) 10.2.2.2/2(L) 10.2.2.2/0(F)
```
The table below describes the significant fields shown in the display.

**Table 61: show ipv6 ospf statistics Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>OSPF area ID.</td>
</tr>
<tr>
<td>SPF</td>
<td>Number of SPF algorithms executed in the OSPF area. The number increases by one for each SPF algorithm that is executed in the area.</td>
</tr>
<tr>
<td>Executed ago</td>
<td>Time in milliseconds that has passed between the start of the SPF algorithm execution and the current time.</td>
</tr>
<tr>
<td>SPF type</td>
<td>SPF type can be Full or Incremental.</td>
</tr>
<tr>
<td>SPT</td>
<td>Time in milliseconds required to compute the first stage of the SPF algorithm (to build a short path tree). The SPT time plus the time required to process links to stub networks equals the Intra time.</td>
</tr>
<tr>
<td>Ext</td>
<td>Time in milliseconds for the SPF algorithm to process external and not so stubby area (NSSA) LSAs and to install external and NSSA routes in the routing table.</td>
</tr>
<tr>
<td>Total</td>
<td>Total duration time in milliseconds for the SPF algorithm process.</td>
</tr>
<tr>
<td>LSIDs processed</td>
<td>Number of LSAs processed during the SPF calculation:</td>
</tr>
<tr>
<td></td>
<td>• N--Network LSA.</td>
</tr>
<tr>
<td></td>
<td>• R--Router LSA.</td>
</tr>
<tr>
<td></td>
<td>• SA--Summary Autonomous System Boundary Router (ASBR) (SA) LSA.</td>
</tr>
<tr>
<td></td>
<td>• SN--Summary Network (SN) LSA.</td>
</tr>
<tr>
<td></td>
<td>• Stub--Stub links.</td>
</tr>
<tr>
<td></td>
<td>• X7--External Type-7 (X7) LSA.</td>
</tr>
</tbody>
</table>
show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPF process, use the **show ipv6 ospf summary-prefix** command in user EXEC or privileged EXEC mode.

```
show ipv6 ospf [process-id] summary-prefix
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when the OSPF routing process is enabled.</td>
</tr>
</tbody>
</table>

### Command Modes

- User EXEC (>
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `process-id` argument can be entered as a decimal number or as an IPv6 address format.

### Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
Device# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

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

### Table 62: show ipv6 ospf summary-prefix Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 Process</td>
<td>Process ID of the router for which information is displayed.</td>
</tr>
<tr>
<td>Metric</td>
<td>Metric used to reach the destination router.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of link-state advertisement (LSA).</td>
</tr>
<tr>
<td>Tag</td>
<td>LSA tag.</td>
</tr>
</tbody>
</table>
**show ipv6 ospf timers rate-limit**

To display all of the link-state advertisements (LSAs) in the rate limit queue, use the `show ipv6 ospf timers rate-limit` command in privileged EXEC mode.

```
show ipv6 ospf timers rate-limit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 ospf timers rate-limit` command to discover when LSAs in the queue will be sent.

**Examples**

**show ipv6 ospf timers rate-limit Output Example**

The following is sample output from the `show ipv6 ospf timers rate-limit` command:

```
Device# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
   LSAID: 0.0.0.0 Type: 0x2001 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
   LSAID: 0.0.0.0 Type: 0x2009 Adv Rtr: 55.55.55.55 Due in: 00:00:00.500
```

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

**Table 63: show ipv6 ospf timers rate-limit Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSAID</td>
<td>ID of the LSA.</td>
</tr>
<tr>
<td>Type</td>
<td>Type of LSA.</td>
</tr>
<tr>
<td>Adv Rtr</td>
<td>ID of the advertising router.</td>
</tr>
<tr>
<td>Due in</td>
<td>When the LSA is scheduled to be sent (in hours:minutes:seconds).</td>
</tr>
</tbody>
</table>
show ipv6 ospf traffic

To display IPv6 Open Shortest Path First Version 3 (OSPFv3) traffic statistics, use the **show ipv6 ospf traffic** command in privileged EXEC mode.

```
show ipv6 ospf [process-id] traffic [interface-type interface-number]
```

**Syntax Description**

- `process-id` (Optional) OSPF process ID for which you want traffic statistics (for example, queue statistics, statistics for each interface under the OSPF process, and per OSPF process statistics).
- `interface-type interface-number` (Optional) Type and number associated with a specific OSPF interface.

**Command Default**

When the **show ipv6 ospf traffic** command is entered without any arguments, global OSPF traffic statistics are displayed, including queue statistics for each OSPF process, statistics for each interface, and per OSPF process statistics.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can limit the displayed traffic statistics to those for a specific OSPF process by entering a value for the `process-id` argument, or you can limit output to traffic statistics for a specific interface associated with an OSPF process by entering values for the `interface-type` and `interface-number` arguments. To reset counters and clear statistics, use the **clear ipv6 ospf traffic** command.

**Examples**

The following example shows the display output for the **show ipv6 ospf traffic** command for OSPFv3:

```
Device# show ipv6 ospf traffic
OSPFv3 statistics:
 Rcvd: 32 total, 0 checksum errors
   10 hello, 7 database desc, 2 link state req
   9 link state updates, 4 link state acks
   0 LSA ignored
 Sent: 45 total, 0 failed
   17 hello, 12 database desc, 2 link state req
   8 link state updates, 6 link state acks
 OSPFv3 Router with ID (10.1.1.4) (Process ID 6)
OSPFv3 queues statistic for process ID 6
   Hello queue size 0, no limit, max size 2
   Router queue size 0, limit 200, drops 0, max size 2
Interface statistics:
   Interface Serial2/0
OSPFv3 packets received/sent
   Type       Packets  Bytes
   RX Invalid 0          0
   RX Hello   5          196
   RX DB des  4          172
```
show ipv6 ospf traffic

OSPFV3 packets received/sent

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>6</td>
<td>240</td>
</tr>
<tr>
<td>RX DB des</td>
<td>3</td>
<td>144</td>
</tr>
<tr>
<td>RX LS req</td>
<td>1</td>
<td>52</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>5</td>
<td>372</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>2</td>
<td>152</td>
</tr>
<tr>
<td>RX Total</td>
<td>17</td>
<td>960</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>11</td>
<td>420</td>
</tr>
<tr>
<td>TX DB des</td>
<td>9</td>
<td>312</td>
</tr>
<tr>
<td>TX LS req</td>
<td>1</td>
<td>52</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>5</td>
<td>376</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>3</td>
<td>148</td>
</tr>
<tr>
<td>TX Total</td>
<td>29</td>
<td>1308</td>
</tr>
</tbody>
</table>

OSPFV3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,

OSPFV3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,

Summary traffic statistics for process ID 6:

OSPFV3 packets received/sent

<table>
<thead>
<tr>
<th>Type</th>
<th>Packets</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RX Invalid</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RX Hello</td>
<td>11</td>
<td>436</td>
</tr>
<tr>
<td>RX DB des</td>
<td>7</td>
<td>316</td>
</tr>
<tr>
<td>RX LS req</td>
<td>2</td>
<td>104</td>
</tr>
<tr>
<td>RX LS upd</td>
<td>9</td>
<td>692</td>
</tr>
<tr>
<td>RX LS ack</td>
<td>4</td>
<td>264</td>
</tr>
<tr>
<td>RX Total</td>
<td>33</td>
<td>1812</td>
</tr>
<tr>
<td>TX Failed</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>TX Hello</td>
<td>19</td>
<td>724</td>
</tr>
<tr>
<td>TX DB des</td>
<td>12</td>
<td>456</td>
</tr>
<tr>
<td>TX LS req</td>
<td>2</td>
<td>104</td>
</tr>
<tr>
<td>TX LS upd</td>
<td>8</td>
<td>628</td>
</tr>
<tr>
<td>TX LS ack</td>
<td>6</td>
<td>296</td>
</tr>
<tr>
<td>TX Total</td>
<td>47</td>
<td>2208</td>
</tr>
</tbody>
</table>

OSPFV3 header errors
Length 0, Checksum 0, Version 0, No Virtual Link 0,
Area Mismatch 0, Self Originated 0, Duplicate ID 0,
Instance ID 0, Hello 0, MTU Mismatch 0,
Nbr Ignored 0, Authentication 0,
OSPFv3 LSA errors
Type 0, Length 0, Data 0, Checksum 0,

The network administrator wants to start collecting new statistics, resetting the counters and clearing the traffic statistics by entering the clear ipv6 ospf traffic command as follows:

Device# clear ipv6 ospf traffic

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPFv3 statistics</td>
<td>Traffic statistics accumulated for all OSPF processes running on the router. To ensure compatibility with the show ip traffic command, only checksum errors are displayed. Identifies the route map name.</td>
</tr>
<tr>
<td>OSPFv3 queues statistic for process ID</td>
<td>Queue statistics specific to Cisco IOS software.</td>
</tr>
<tr>
<td>Hello queue</td>
<td>Statistics for the internal Cisco IOS queue between the packet switching code (process IP Input) and the OSPF hello process for all received OSPF packets.</td>
</tr>
<tr>
<td>Router queue</td>
<td>Statistics for the internal Cisco IOS queue between the OSPF hello process and the OSPF router for all received OSPF packets except OSPF hellos.</td>
</tr>
<tr>
<td>queue size</td>
<td>Actual size of the queue.</td>
</tr>
<tr>
<td>queue limit</td>
<td>Maximum allowed size of the queue.</td>
</tr>
<tr>
<td>queue max size</td>
<td>Maximum recorded size of the queue.</td>
</tr>
<tr>
<td>Interface statistics</td>
<td>Per-interface traffic statistics for all interfaces that belong to the specific OSPFv3 process ID.</td>
</tr>
<tr>
<td>OSPFv3 packets received/sent</td>
<td>Number of OSPFv3 packets received and sent on the interface, sorted by packet types.</td>
</tr>
<tr>
<td>OSPFv3 header errors</td>
<td>Packet appears in this section if it was discarded because of an error in the header of an OSPFv3 packet. The discarded packet is counted under the appropriate discard reason.</td>
</tr>
<tr>
<td>OSPFv3 LSA errors</td>
<td>Packet appears in this section if it was discarded because of an error in the header of an OSPF link-state advertisement (LSA). The discarded packet is counted under the appropriate discard reason.</td>
</tr>
<tr>
<td>Summary traffic statistics for process ID</td>
<td>Summary traffic statistics accumulated for an OSPFv3 process.</td>
</tr>
</tbody>
</table>

Note: The OSPF process ID is a unique value assigned to the OSPFv3 process in the configuration.

The value for the received errors is the sum of the OSPFv3 header errors that are detected by the OSPFv3 process, unlike the sum of the checksum errors that are listed in the global OSPF statistics.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip ospf traffic</td>
<td>Clears OSPFv2 traffic statistics.</td>
</tr>
<tr>
<td>clear ipv6 ospf traffic</td>
<td>Clears OSPFv3 traffic statistics.</td>
</tr>
<tr>
<td>show ip ospf traffic</td>
<td>Displays OSPFv2 traffic statistics.</td>
</tr>
</tbody>
</table>
show ipv6 ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the `show ipv6 ospf virtual-links` command in user EXEC or privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

- User EXEC (`->`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The information displayed by the `show ipv6 ospf virtual-links` command is useful in debugging OSPF routing operations.

**Examples**

The following is sample output from the `show ipv6 ospf virtual-links` command:

```
Device# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:06
```

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

**Table 65: show ipv6 ospf virtual-links Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Link OSPF_VL0 to router 172.16.6.6 is up</td>
<td>Specifies the OSPF neighbor, and if the link to that neighbor is up or down.</td>
</tr>
<tr>
<td>Interface ID</td>
<td>Interface ID and IPv6 address of the router.</td>
</tr>
<tr>
<td>Transit area 2</td>
<td>The transit area through which the virtual link is formed.</td>
</tr>
<tr>
<td>via interface ATM3/0</td>
<td>The interface through which the virtual link is formed.</td>
</tr>
<tr>
<td>Cost of using 1</td>
<td>The cost of reaching the OSPF neighbor through the virtual link.</td>
</tr>
<tr>
<td>Transmit Delay is 1 sec</td>
<td>The transmit delay (in seconds) on the virtual link.</td>
</tr>
<tr>
<td>State POINT_TO_POINT</td>
<td>The state of the OSPF neighbor.</td>
</tr>
</tbody>
</table>
The various timer intervals configured for the link.

When the next hello is expected from the neighbor.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer intervals...</td>
<td>The various timer intervals configured for the link.</td>
</tr>
<tr>
<td>Hello due in 0:00:06</td>
<td>When the next hello is expected from the neighbor.</td>
</tr>
</tbody>
</table>

The following sample output from the `show ipv6 ospf virtual-links` command has two virtual links. One is protected by authentication, and the other is protected by encryption.

```
Device# show ipv6 ospf virtual-links
Virtual Link OSPFv3_VL1 to router 10.2.0.1 is up
  Interface ID 69, IPv6 address 2001:0DB8:11:0:A8BB:CCFF:FE00:6A00
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial12/0, Cost of using 64
  NULL encryption SHA-1 auth SPI 3944, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 2, Dead 10, Wait 40, Retransmit 5
  Adjacency State FULL (Hello suppressed)
  Index 1/2/4, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec

Virtual Link OSPFv3_VL0 to router 10.1.0.1 is up
  Interface ID 67, IPv6 address 2001:0DB8:13:0:A8BB:CCFF:FE00:6700
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial11/0, Cost of using 128
  MD5 authentication SPI 940, secure socket UP (errors: 0)
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Adjacency State FULL (Hello suppressed)
  Index 1/1/3, retransmission queue length 0, number of retransmission 1
  First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
  Last retransmission scan length is 1, maximum is 1
  Last retransmission scan time is 0 msec, maximum is 0 msec
```
show ipv6 pim anycast-RP

To verify IPv6 PIM anycast RP operation, use the `show ipv6 pim anycast-RP` command in user EXEC or privileged EXEC mode.

```
show ipv6 pim anycast-RP rp-address
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th><code>rp-address</code></th>
<th>RP address to be verified.</th>
</tr>
</thead>
</table>

**Command Modes**

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC (&gt;)</td>
</tr>
<tr>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Examples**

```
Device# show ipv6 pim anycast-rp 110::1:1

Anycast RP Peers For 110::1:1:1 Last Register/Register-Stop received 20::1:1:1 00:00:00/00:00:00
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 pim anycast-RP</td>
<td>Configures the address of the PIM RP for an anycast group range.</td>
</tr>
</tbody>
</table>
**show ipv6 pim bsr**

To display information related to Protocol Independent Multicast (PIM) bootstrap router (BSR) protocol processing, use the `show ipv6 pim bsr` command in user EXEC or privileged EXEC mode.

`show ipv6 pim [vrf vrf-name] bsr {election | rp-cache | candidate-rp}`

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>election</td>
<td>Displays BSR state, BSR election, and bootstrap message (BSM)-related timers.</td>
</tr>
<tr>
<td>rp-cache</td>
<td>Displays candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.</td>
</tr>
<tr>
<td>candidate-rp</td>
<td>Displays C-RP state on devices that are configured as C-RPs.</td>
</tr>
</tbody>
</table>

### Command Modes

- User EXEC (>
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show ipv6 pim bsr` command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP cache is displayed only on the elected BSR device, and information on the C-RP state machine is displayed only on a device configured as a C-RP.

### Examples

The following example displays BSM election information:

```
Device# show ipv6 pim bsr election
PIMv2 BSR information
BSR Election Information
Scope Range List: ff00::/8
This system is the Bootstrap Router (BSR)
BSR Address: 60::1:1:4
Uptime: 00:11:55, BSR Priority: 0, Hash mask length: 126
RPF: FE80::A8BB:CCFF:FE03:C400, Ethernet0/0
BS Timer: 00:00:07
This system is candidate BSR
Candidate BSR address: 60::1:1:4, priority: 0, hash mask length: 126
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope Range List</td>
<td>Scope to which this BSR information applies.</td>
</tr>
</tbody>
</table>
Indicate this device is the Bootstrap Router (BSR)

This system is the Bootstrap Router (BSR)

Indicates this device is the BSR and provides information on the parameters associated with it.

On the elected BSR, the BS timer shows the time in which the next BSM will be originated.

On all other devices in the domain, the BS timer shows the time at which the elected BSR expires.

Indicates this device is the candidate BSR and provides information on the parameters associated with it.

The following example displays information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range:

```
Device# show ipv6 pim bsr rp-cache
PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8, RP count 2
    RP 10::1:1:3
      Priority 192, Holdtime 150
      Uptime: 00:12:36, expires: 00:01:55
    RP 20::1:1:1
      Priority 192, Holdtime 150
      Uptime: 00:12:36, expires: 00:01:5
```

The following example displays information about the C-RP. This RP has been configured without a specific scope value, so the RP will send C-RP advertisements to all BSRs about which it has learned through BSMs it has received.

```
Device# show ipv6 pim bsr candidate-rp
PIMv2 C-RP information
    Candidate RP: 10::1:1:3
      All Learnt Scoped Zones, Priority 192, Holdtime 150
      Advertisement interval 60 seconds
      Next advertisement in 00:00:33
```

The following example confirms that the IPv6 C-BSR is PIM-enabled. If PIM is disabled on an IPv6 C-BSR interface, or if a C-BSR or C-RP is configured with the address of an interface that does not have PIM enabled, the `show ipv6 pim bsr election` command used with the `election` keyword would display that information instead.

```
Device# show ipv6 pim bsr election
PIMv2 BSR information
    BSR Election Information
      Scope Range List: ff00::/8
      BSR Address: 2001:DB8:1:1:2
      Uptime: 00:02:42, BSR Priority: 34, Hash mask length: 28
      RPF: FE80::20:1:2, Ethernet1/0
      BS Timer: 00:01:27
```
show ipv6 pim df

To display the designated forwarder (DF)-election state of each interface for each rendezvous point (RP), use the `show ipv6 pim df` command in user EXEC or privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] df [interface-type interface-number] [rp-address]
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface-type</td>
<td>interface-number</td>
<td>(Optional) Interface type and number. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>rp-address</td>
<td></td>
<td>(Optional) RP IPv6 address.</td>
</tr>
</tbody>
</table>

Command Default

If no interface or RP address is specified, all DFs are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use the `show ipv6 pim df` command to display the state of the DF election for each RP on each Protocol Independent Multicast (PIM)-enabled interface if the bidirectional multicast traffic is not flowing as expected.

Examples

The following example displays the DF-election states:

```
Device# show ipv6 pim df
Interface  DF State  Timer    Metrics
Ethernet0/0  Winner  4s 8ms  [120/2]
  RP :200::1
Ethernet1/0  Lose   0s 0ms  [inf/inf]
  RP :200::1
```

The following example shows information on the RP:

```
Device# show ipv6 pim df
Interface  DF State  Timer    Metrics
Ethernet0/0  None:RP LAN 0s 0ms  [inf/inf]
  RP :200::1
Ethernet1/0  Winner  7s 600ms  [0/0]
  RP :200::1
Ethernet2/0  Winner  9s 8ms  [0/0]
  RP :200::1
```

The table below describes the significant fields shown in the display.
### Table 67: `show ipv6 pim df` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type and number that is configured to run PIM.</td>
</tr>
<tr>
<td>DF State</td>
<td>The state of the DF election on the interface. The state can be:</td>
</tr>
<tr>
<td></td>
<td>• Offer</td>
</tr>
<tr>
<td></td>
<td>• Winner</td>
</tr>
<tr>
<td></td>
<td>• Backoff</td>
</tr>
<tr>
<td></td>
<td>• Lose</td>
</tr>
<tr>
<td></td>
<td>• None:RP LAN</td>
</tr>
<tr>
<td>Timer</td>
<td>DF election timer.</td>
</tr>
<tr>
<td>Metrics</td>
<td>Routing metrics to the RP announced by the DF.</td>
</tr>
<tr>
<td>RP</td>
<td>The IPv6 address of the RP.</td>
</tr>
</tbody>
</table>

The `None:RP LAN` state indicates that no DF election is taking place on this LAN because the RP is directly connected to this LAN.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ipv6 pim df-election</code></td>
<td>Displays debug messages for PIM bidirectional DF-election message processing.</td>
</tr>
<tr>
<td><code>ipv6 pim rp-address</code></td>
<td>Configures the address of a PIM RP for a particular group range.</td>
</tr>
<tr>
<td><code>show ipv6 pim df winner</code></td>
<td>Displays the DF-election winner on each interface for each RP.</td>
</tr>
</tbody>
</table>
**show ipv6 pim group-map**

To display an IPv6 Protocol Independent Multicast (PIM) group mapping table, use the `show ipv6 pim group-map` command in user EXEC or privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] group-map [{group-name|group-address}] [{group-range|group-mask}] [info-source {bsr | default | embedded-rp | static}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>group-range</td>
<td>(Optional) Group range list. Includes group ranges with the same prefix or mask length.</td>
</tr>
<tr>
<td>group-mask</td>
<td>(Optional) Group range list. Includes group ranges with the same prefix or mask length.</td>
</tr>
<tr>
<td>info-source</td>
<td>(Optional) Displays all mappings learned from a specific source, such as the bootstrap router (BSR) or static configuration.</td>
</tr>
<tr>
<td>bsr</td>
<td>Displays ranges learned through the BSR.</td>
</tr>
<tr>
<td>default</td>
<td>Displays ranges enabled by default.</td>
</tr>
<tr>
<td>embedded-rp</td>
<td>Displays group ranges learned through the embedded rendezvous point (RP).</td>
</tr>
<tr>
<td>static</td>
<td>Displays ranges enabled by static configuration.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 pim group-map` command to find all group mappings installed by a given source of information, such as BSR or static configuration.

You can also use this command to find which group mapping a router at a specified IPv6 group address is using by specifying a group address, or to find an exact group mapping entry by specifying a group range and mask length.

**Examples**

The following is sample output from the `show ipv6 pim group-map` command:

```
Device# show ipv6 pim group-map
FF33::/32*
    SSM
    Info source:Static
    Uptime:00:08:32, Groups:0
FF34::/32*
    SSM
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The table below describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP</td>
<td>Address of the RP router if the protocol is sparse mode or bidir.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol used: sparse mode (SM), Source Specific Multicast (SSM), link-local (LL), or NOROUTE (NO). LL is used for the link-local scoped IPv6 address range (ff0-f::/16). LL is treated as a separate protocol type, because packets received with these destination addresses are not forwarded, but the router might need to receive and process them. NOROUTE or NO is used for the reserved and node-local scoped IPv6 address range (ff0-f][0-1]::/16). These addresses are nonroutable, and the router does not need to process them.</td>
</tr>
<tr>
<td>Groups</td>
<td>How many groups are present in the topology table from this range.</td>
</tr>
<tr>
<td>Info source</td>
<td>Mappings learned from a specific source; in this case, static configuration.</td>
</tr>
<tr>
<td>Uptime</td>
<td>The uptime for the group mapping displayed.</td>
</tr>
</tbody>
</table>

The following example displays the group mappings learned from BSRs that exist in the PIM group-to-RP or mode-mapping cache. The example shows the address of the BSR from which the group mappings have been learned and the associated timeout.

```
Router# show ipv6 pim group-map info-source bsr
FF00::/8*
  SM, RP: 20::1:1:1
  RPF: Et1/0, FE80::A8BB:CCFF:FE03:C202
  Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
  Uptime: 00:19:51, Groups: 0
FF00::/8*
  SM, RP: 10::1:1:3
  RPF: Et0/0, FE80::A8BB:CCFF:FE03:C102
  Info source: BSR From: 60::1:1:4(00:01:42), Priority: 192
  Uptime: 00:19:51, Groups: 0
```
show ipv6 pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the `show ipv6 pim interface` command in privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] interface [state-on] [state-off] [type number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>state-on</td>
<td>(Optional) Displays interfaces with PIM enabled.</td>
</tr>
<tr>
<td>state-off</td>
<td>(Optional) Displays interfaces with PIM disabled.</td>
</tr>
<tr>
<td>type number</td>
<td>(Optional) Interface type and number.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 pim interface` command is used to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface.

**Examples**

The following is sample output from the `show ipv6 pim interface` command using the `state-on` keyword:

```
Device# show ipv6 pim interface state-on
Interface     PIM Nbr Hello DR
Count Intvl Prior
Ethernet0     on  0   30  1
    Address:FE80::208:2FF:FE08:D7FF
    DR :this system
POS1/0        on  0   30  1
    Address:FE80::208:2FF:FE08:D554
    DR :this system
POS4/0        on  1   30  1
    Address:FE80::208:2FF:FE08:D554
    DR :this system
POS4/1        on  0   30  1
    Address:FE80::208:2FF:FE08:D554
    DR :this system
Loopback0     on  0   30  1
    Address:FE80::208:2FF:FE08:D554
    DR :this system
```

The table below describes the significant fields shown in the display.
Table 69: show ipv6 pim interface Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type and number that is configured to run PIM.</td>
</tr>
<tr>
<td>PIM</td>
<td>Whether PIM is enabled on an interface.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Number of PIM neighbors that have been discovered through this interface.</td>
</tr>
<tr>
<td>Hello Intvl</td>
<td>Frequency, in seconds, of PIM hello messages.</td>
</tr>
<tr>
<td>DR Address</td>
<td>IP address of the designated router (DR) on a network.</td>
</tr>
<tr>
<td>Address</td>
<td>Interface IP address of the next-hop router.</td>
</tr>
</tbody>
</table>

The following is sample output from the **show ipv6 pim interface** command, modified to display passive interface information:

```
Device(config)# show ipv6 pim interface gigabitethernet0/0/0

Interface PIM Nbr Hello DR BFD
Count Intvl Prior

GigabitEthernet0/0/0 on/P 0 30 1 On
Address: FE80::A8BB:CCFF:FE00:9100
DR : this system
```

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

Table 70: show ipv6 pim interface Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIM</td>
<td>Whether PIM is enabled on an interface. When PIM passive mode is used, a &quot;P&quot; is displayed in the output.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 pim neighbor</td>
<td>Displays the PIM neighbors discovered by the Cisco IOS software.</td>
</tr>
</tbody>
</table>
show ipv6 pim join-prune statistic

To display the average join-prune aggregation for the most recently aggregated 1000, 10,000, and 50,000 packets for each interface, use the **show ipv6 pim join-prune statistic** command in user EXEC or privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] join-prune statistic [interface-type]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When Protocol Independent Multicast (PIM) sends multiple joins and prunes simultaneously, it aggregates them into a single packet. The **show ipv6 pim join-prune statistic** command displays the average number of joins and prunes that were aggregated into a single packet over the last 1000 PIM join-prune packets, over the last 10,000 PIM join-prune packets, and over the last 50,000 PIM join-prune packets.

**Examples**

The following example provides the join/prune aggregation on Ethernet interface 0/0/0:

```
Device# show ipv6 pim join-prune statistic Ethernet0/0/0
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface Transmitted Received
Ethernet0/0/0 0 / 0 / 0 1 / 0 / 0
```

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

**Table 71: show ipv6 pim join-prune statistics Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface from which the specified packets were transmitted or on which they were received.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>The number of packets transmitted on the interface.</td>
</tr>
<tr>
<td>Received</td>
<td>The number of packets received on the interface.</td>
</tr>
</tbody>
</table>
show ipv6 pim limit

To display Protocol Independent Multicast (PIM) interface limit, use the show ipv6 pim limit command in privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] limit [interface]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Specific interface for which limit information is provided.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The show ipv6 pim limit command checks interface statistics for limits. If the optional interface argument is enabled, only information for the specified interface is shown.

**Examples**

The following example displays PIM interface limit information:

```
Device# show ipv6 pim limit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 multicast limit</td>
<td>Configures per-interface mroute state limiters in IPv6.</td>
</tr>
<tr>
<td>ipv6 multicast limit cost</td>
<td>Applies a cost to mroutes that match per interface mroute state limiters in IPv6.</td>
</tr>
</tbody>
</table>
show ipv6 pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco software, use the `show ipv6 pim neighbor` command in privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name ]neighbor [detail ][[interface-type interface-number | count]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the additional addresses of the neighbors learned, if any, through the routable address hello option.</td>
</tr>
<tr>
<td>interface-type interface-number</td>
<td>(Optional) Interface type and number.</td>
</tr>
<tr>
<td>count</td>
<td>(Optional) Displays neighbor counts on each interface.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 pim neighbor` command displays which routers on the LAN are configured for PIM.

**Examples**

The following is sample output from the `show ipv6 pim neighbor` command using the detail keyword to identify the additional addresses of the neighbors learned through the routable address hello option:

```
Device#  show ipv6 pim neighbor detail
Neighbor Address(es)     Interface     Uptime     Expires    DR    pri Bidir
FE80::A8BB:CCFF:FE00:401 Ethernet0/0     01:34:16     00:01:16 1    B
60::1:1:3
FE80::A8BB:CCFF:FE00:501 Ethernet0/0     01:34:15     00:01:18 1    B
60::1:1:4
```

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

**Table 72: show ipv6 pim neighbor Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor addresses</td>
<td>IPv6 address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface type and number on which the neighbor is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>How long (in hours, minutes, and seconds) the entry has been in the PIM neighbor table.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expires</td>
<td>How long (in hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table.</td>
</tr>
<tr>
<td>DR</td>
<td>Indicates that this neighbor is a designated router (DR) on the LAN.</td>
</tr>
<tr>
<td>pri</td>
<td>DR priority used by this neighbor.</td>
</tr>
<tr>
<td>Bidir</td>
<td>The neighbor is capable of PIM in bidirectional mode.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 pim interfaces</code></td>
<td>Displays information about interfaces configured for PIM.</td>
</tr>
</tbody>
</table>
show ipv6 pim range-list

To display information about IPv6 multicast range lists, use the **show ipv6 pim range-list** command in privileged EXEC mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td><code>config</code></td>
<td>(Optional) The client. Displays the range lists configured on the router.</td>
</tr>
<tr>
<td>`rp-address</td>
<td>rp-name`</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show ipv6 pim range-list** command displays IPv6 multicast range lists on a per-client and per-mode basis. A client is the entity from which the specified range list was learned. The clients can be config, and the modes can be Source Specific Multicast (SSM) or sparse mode (SM).

**Examples**

The following is sample output from the **show ipv6 pim range-list** command:

```
Device# show ipv6 pim range-list
config SSM Exp:never Learnt from :::
FF33::/32 Up:00:26:33
FF34::/32 Up:00:26:33
FF35::/32 Up:00:26:33
FF36::/32 Up:00:26:33
FF37::/32 Up:00:26:33
FF38::/32 Up:00:26:33
FF39::/32 Up:00:26:33
FF3A::/32 Up:00:26:33
FF3B::/32 Up:00:26:33
FF3C::/32 Up:00:26:33
FF3D::/32 Up:00:26:33
FF3E::/32 Up:00:26:33
FF3F::/32 Up:00:26:33
config SM RP:40::1:1:1 Exp:never Learnt from :::
FF13::/64 Up:00:26:33
config SM RP:40::1:1:3 Exp:never Learnt from :::
FF09::/64 Up:00:03:50
```

The table below describes the significant fields shown in the display.
**Table 73: show ipv6 pim range-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Config is the client.</td>
</tr>
<tr>
<td>SSM</td>
<td>Protocol being used.</td>
</tr>
<tr>
<td>FF33::/32</td>
<td>Group range.</td>
</tr>
<tr>
<td>Up:</td>
<td>Uptime.</td>
</tr>
</tbody>
</table>
**show ipv6 pim topology**

To display Protocol Independent Multicast (PIM) topology table information for a specific group or all groups, use the `show ipv6 pim topology` command in user EXEC or privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] topology [{group-name | group-address} [{source-address | source-name}] | link-local] route-count [detail]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>group-name</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) IPv6 address or name of the multicast group.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) IPv6 address or name of the source.</td>
</tr>
<tr>
<td>source-name</td>
<td>(Optional) IPv6 address or name of the source.</td>
</tr>
<tr>
<td>link-local</td>
<td>(Optional) Displays the link-local groups.</td>
</tr>
<tr>
<td>route-count</td>
<td>(Optional) Displays the number of routes in PIM topology table.</td>
</tr>
</tbody>
</table>

### Command Modes

- User EXEC (`>`)
- Privileged EXEC (`#`)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command shows the PIM topology table for a given group--(*, G), (S, G), and (S, G) Rendezvous Point Tree (RPT)-- as internally stored in a PIM topology table. The PIM topology table may have various entries for a given group, each with its own interface list. The resulting forwarding state is maintained in the Multicast Routing Information Base (MRIB) table, which shows which interface the data packet should be accepted on and which interfaces the data packet should be forwarded to for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

The `route-count` keyword shows the count of all entries, including link-local entries.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols (such as PIM), local membership protocols (such as Multicast Listener Discovery [MLD]), and the multicast forwarding engine of the system.

For example, an interface is added to the (*, G) entry in PIM topology table upon receipt of an MLD report or PIM (*, G) join message. Similarly, an interface is added to the (S, G) entry upon receipt of the MLD INCLUDE report for the S and G or PIM (S, G) join message. Then PIM installs an (S, G) entry in the MRIB with the immediate olist (from (S, G)) and the inherited olist (from (*, G)). Therefore, the proper forwarding state for a given entry (S, G) can be seen only in the MRIB or the MFIB, not in the PIM topology table.

### Examples

The following is sample output from the `show ipv6 pim topology` command:

```
Device# show ipv6 pim topology
```
The table below describes the significant fields shown in the display.

**Table 74: show ipv6 pim topology Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry flags: KAT</td>
<td>The keepalive timer (KAT) associated with a source is used to keep track of two intervals while the source is alive. When a source first becomes active, the first-hop router sets the keepalive timer to 3 minutes and 30 seconds, during which time it does not probe to see if the source is alive. Once this timer expires, the router enters the probe interval and resets the timer to 65 seconds, during which time the router assumes the source is alive and starts probing to determine if it actually is. If the router determines that the source is alive, the router exits the probe interval and resets the keepalive timer to 3 minutes and 30 seconds. If the source is not alive, the entry is deleted at the end of the probe interval.</td>
</tr>
<tr>
<td>AA, PA</td>
<td>The assume alive (AA) and probe alive (PA) flags are set when the router is in the probe interval for a particular source.</td>
</tr>
<tr>
<td>RR</td>
<td>The register received (RR) flag is set on the (S, G) entries on the Route Processor (RP) as long as the RP receives registers from the source Designated Router (DR), which keeps the source state alive on the RP.</td>
</tr>
<tr>
<td>SR</td>
<td>The sending registers (SR) flag is set on the (S, G) entries on the DR as long as it sends registers to the RP.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ipv6 mrib client</td>
<td>Displays information about the clients of the MRIB.</td>
</tr>
<tr>
<td>show ipv6 mrib route</td>
<td>Displays MRIB route information.</td>
</tr>
</tbody>
</table>
show ipv6 pim traffic

To display the Protocol Independent Multicast (PIM) traffic counters, use the `show ipv6 pim traffic` command in user EXEC or privileged EXEC mode.

```
show ipv6 pim [vrf vrf-name] traffic
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a virtual routing and forwarding (VRF) configuration.

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ipv6 pim traffic` command to check if the expected number of PIM protocol messages have been received and sent.

**Examples**

The following example shows the number of PIM protocol messages received and sent.

```
Device# show ipv6 pim traffic
PIM Traffic Counters
Elapsed time since counters cleared:00:05:29
Received    Sent
Valid PIM Packets  22   22
Hello          22   22
Join-Prune     0    0
Register       0    0
Register Stop  0    0
Assert         0    0
Bidir DF Election 0   0
Errors:
Malformed Packets  0
Bad Checksums    0
Send Errors      0
Packet Sent on Loopback Errors 0
Packets Received on PIM-disabled Interface 0
Packets Received with Unknown PIM Version 0

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

**Table 75: show ipv6 pim traffic Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since counters cleared</td>
<td>Indicates the amount of time (in hours, minutes, and seconds) since the counters cleared.</td>
</tr>
<tr>
<td>Valid PIM Packets</td>
<td>Number of valid PIM packets received and sent.</td>
</tr>
</tbody>
</table>
**Field** | **Description**  
--- | ---  
Hello | Number of valid hello messages received and sent.  
Join-Prune | Number of join and prune announcements received and sent.  
Register | Number of PIM register messages received and sent.  
Register Stop | Number of PIM register stop messages received and sent.  
Assert | Number of asserts received and sent.
show ipv6 pim tunnel

To display information about the Protocol Independent Multicast (PIM) register encapsulation and de-encapsulation tunnels on an interface, use the **show ipv6 pim tunnel** command in privileged EXEC mode.

```
show_ipv6_pim_tunnel [vrf vrf-name] tunnel [interface-type interface-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Tunnel interface type and number.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you use the **show ipv6 pim tunnel** command without the optional `interface` keyword, information about the PIM register encapsulation and de-encapsulation tunnel interfaces is displayed.

The PIM encapsulation tunnel is the register tunnel. An encapsulation tunnel is created for every known rendezvous point (RP) on each router. The PIM decapsulation tunnel is the register decapsulation tunnel. A decapsulation tunnel is created on the RP for the address that is configured to be the RP address.

**Examples**

The following is sample output from the **show ipv6 pim tunnel** command on the RP:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type : PIM Encap
  RP : 100::1
  Source: 100::1
Tunnel0*
  Type : PIM Decap
  RP : 100::1
  Source: -
```

The following is sample output from the **show ipv6 pim tunnel** command on a non-RP:

```
Device# show ipv6 pim tunnel
Tunnel0*
  Type : PIM Encap
  RP : 100::1
  Source: 2001::1:1:1
```

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

**Table 76: show ipv6 pim tunnel Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel0*</td>
<td>Name of the tunnel.</td>
</tr>
</tbody>
</table>
**Field** | **Description**  
--- | ---  
Type | Type of tunnel. Can be PIM encapsulation or PIM de-encapsulation.  
source | Source address of the router that is sending encapsulating registers to the RP.
show ipv6 policy

To display the IPv6 policy-based routing (PBR) configuration, use the `show ipv6 policy` command in user EXEC or privileged EXEC mode.

```
Device# show ipv6 policy
```

### Syntax Description

This command has no arguments or keywords.

### Command Modes

- User EXEC (>
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

IPv6 policy matches will be counted on route maps, as is done in IPv4. Therefore, IPv6 policy matches can also be displayed on the `show route-map` command.

### Examples

The following example displays the PBR configuration:

```
Device# show ipv6 policy

Interface Routemap
Ethernet0/0 src-1
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface type and number that is configured to run Protocol-Independent Multicast (PIM).</td>
</tr>
<tr>
<td>Routemap</td>
<td>The name of the route map on which IPv6 policy matches were counted.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show route-map</code></td>
<td>Displays all route maps configured or only the one specified.</td>
</tr>
</tbody>
</table>
**show ipv6 prefix-list**

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

```
show ipv6 prefix-list [{detail | summary}] [list-name]
show ipv6 prefix-list list-name ipv6-prefix/prefix-length [{longer | first-match}]
show ipv6 prefix-list list-name seq seq-num
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Detail</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Optional) Displays detailed or summarized information about all IPv6 prefix lists.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional) The name of a specific IPv6 prefix list.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given ipv6-prefix / prefix-length values.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Optional) Displays the entry of an IPv6 prefix list that matches the given ipv6-prefix / prefix-length values.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The sequence number of the IPv6 prefix list entry.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

Displays information about all IPv6 prefix lists.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **show ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

**Examples**

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Device# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
```
The table below describes the significant fields shown in the display.

**Table 77: show ipv6 prefix-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefix list with the latest deletion/insertion:</td>
<td>Prefix list that was last modified.</td>
</tr>
<tr>
<td>count</td>
<td>Number of entries in the list.</td>
</tr>
<tr>
<td>range entries</td>
<td>Number of entries with matching range.</td>
</tr>
<tr>
<td>sequences</td>
<td>Sequence number for the prefix entry.</td>
</tr>
<tr>
<td>refcount</td>
<td>Number of objects currently using this prefix list.</td>
</tr>
<tr>
<td>seq</td>
<td>Entry number in the list.</td>
</tr>
<tr>
<td>permit, deny</td>
<td>Granting status.</td>
</tr>
<tr>
<td>hit count</td>
<td>Number of matches for the prefix entry.</td>
</tr>
</tbody>
</table>

The following example shows the output of the `show ipv6 prefix-list` command with the `summary` keyword:

```
Device# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
  count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
  count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
  seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
  seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
  count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
  seq 5 deny 3FFE::/24 ge 25 (hit count: 568, refcount: 1)
  seq 10 deny ::/0 (hit count: 0, refcount: 1)
  seq 15 deny ::/1 (hit count: 0, refcount: 1)
  seq 20 deny ::/2 (hit count: 0, refcount: 1)
  seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
  seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 prefix-list</td>
<td>Resets the hit count of the prefix list entries.</td>
</tr>
<tr>
<td>distribute-list in</td>
<td>Filters networks received in updates.</td>
</tr>
<tr>
<td>distribute-list out</td>
<td>Suppresses networks from being advertised in updates.</td>
</tr>
<tr>
<td>ipv6 prefix-list</td>
<td>Creates an entry in an IPv6 prefix list.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ipv6 prefix-list description</td>
<td>Adds a text description of an IPv6 prefix list.</td>
</tr>
<tr>
<td>match ipv6 address</td>
<td>Distributes IPv6 routes that have a prefix permitted by a prefix list.</td>
</tr>
<tr>
<td>neighbor prefix-list</td>
<td>Distributes BGP neighbor information as specified in a prefix list.</td>
</tr>
<tr>
<td>remark (prefix-list)</td>
<td>Adds a comment for an entry in a prefix list.</td>
</tr>
</tbody>
</table>
**show ipv6 protocols**

To display the parameters and the current state of the active IPv6 routing protocol processes, use the `show ipv6 protocols` command in user EXEC or privileged EXEC mode.

```
show ipv6 protocols [summary]
```

**Syntax Description**

- `summary` (Optional) Displays the configured routing protocol process names.

**Command Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The information displayed by the `show ipv6 protocols` command is useful in debugging routing operations.

**Examples**

The following sample output from the `show ipv6 protocols` command displays Intermediate System-to-Intermediate System (IS-IS) routing protocol information:

```
Device# show ipv6 protocols

IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "static"
IPv6 Routing Protocol is "isis"
Interfaces:
  Ethernet0/0/3
  Ethernet0/0/1
  Serial1/0/1
  Loopback1 (Passive)
  Loopback2 (Passive)
  Loopback3 (Passive)
  Loopback4 (Passive)
  Loopback5 (Passive)
Redistribution:
  Redistributing protocol static at level 1
Inter-area redistribution
  Redistributing L1 into L2 using prefix-list word
Address Summarization:
  L2: 33::/16 advertised with metric 0
  L2: 44::/16 advertised with metric 20
  L2: 66::/16 advertised with metric 10
  L2: 77::/16 advertised with metric 10
```

The table below describes the significant fields shown in the display.
### Table 78: show ipv6 protocols Field Descriptions for IS-IS Processes

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Routing Protocol is</td>
<td>Specifies the IPv6 routing protocol used.</td>
</tr>
<tr>
<td>Interfaces</td>
<td>Specifies the interfaces on which the IPv6 IS-IS protocol is configured.</td>
</tr>
<tr>
<td>Redistribution</td>
<td>Lists the protocol that is being redistributed.</td>
</tr>
<tr>
<td>Inter-area redistribution</td>
<td>Lists the IS-IS levels that are being redistributed into other levels.</td>
</tr>
<tr>
<td>using prefix-list</td>
<td>Names the prefix list used in the interarea redistribution.</td>
</tr>
<tr>
<td>Address Summarization</td>
<td>Lists all the summary prefixes. If the summary prefix is being advertised,</td>
</tr>
<tr>
<td></td>
<td>&quot;advertised with metric x&quot; will be displayed after the prefix.</td>
</tr>
</tbody>
</table>

The following sample output from the `show ipv6 protocols` command displays the Border Gateway Protocol (BGP) information for autonomous system 30:

Device# `show ipv6 protocols`

IPv6 Routing Protocol is "bgp 30"
IGP synchronization is disabled
Redistribution:
  Redistributing protocol connected
  Neighbor(s):
    Address FiltIn FiltOut Weight RoutemapIn RoutemapOut
    2001:DB8:0:ABCD::1 5 7 200 rmap-in rmap-out
    2001:DB8:0:ABCD::2
    2001:DB8:0:ABCD::3

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

### Table 79: show ipv6 protocols Field Descriptions for BGP Process

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Routing Protocol is</td>
<td>Specifies the IPv6 routing protocol used.</td>
</tr>
<tr>
<td>Redistribution</td>
<td>Lists the protocol that is being redistributed.</td>
</tr>
<tr>
<td>Address</td>
<td>Neighbor IPv6 address.</td>
</tr>
<tr>
<td>FiltIn</td>
<td>AS-path filter list applied to input.</td>
</tr>
<tr>
<td>FiltOut</td>
<td>AS-path filter list applied to output.</td>
</tr>
<tr>
<td>Weight</td>
<td>Neighbor weight value used in BGP best path selection.</td>
</tr>
<tr>
<td>RoutemapIn</td>
<td>Neighbor route map applied to input.</td>
</tr>
<tr>
<td>RoutemapOut</td>
<td>Neighbor route map applied to output.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ipv6 protocols summary` command:

Device# `show ipv6 protocols summary`
The following sample output from the `show ipv6 protocols` command displays the EIGRP information including the vector metric and EIGRP IPv6 NSF:

```
Device# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "bgp 1"
  IGP synchronization is disabled
  Redistribution:
    None
IPv6 Routing Protocol is "bgp multicast"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "eigrp 1"
EIGRP-IPv6 VR(name) Address-Family Protocol for AS(1)
  Metric weight K1=1, K2=0, K3=1, K4=0, K5=0 K6=0
  Metric rib-scale 128
  Metric version 64bit
  NSF-aware route hold timer is 260
  EIGRP NSF enabled
    NSF signal timer is 15s
    NSF converge timer is 65s
Router-ID: 10.1.2.2
Topology : 0 (base)
  Active Timer: 3 min
  Distance: internal 90 external 170
  Maximum path: 16
  Maximum hopcount 100
  Maximum metric variance 1
  Total Prefix Count: 0
  Total Redist Count: 0

Interfaces:
Redistribution:
  None
```

The following example displays IPv6 protocol information after configuring redistribution in an Open Shortest Path First (OSPF) domain:

```
Device# redistribute ospf 1 match internal
Device(config-rtr)# end
Device# show ipv6 protocols
IPv6 Routing Protocol is "connected"
IPv6 Routing Protocol is "ND"
IPv6 Routing Protocol is "rip 1"
Interfaces:
  Ethernet0/1
  Loopback9
Redistribution:
  Redistributing protocol ospf 1 (internal)
IPv6 Routing Protocol is "ospf 1"
Interfaces (Area 0):
  Ethernet0/0
Redistribution:
  None
```
show ipv6 rip

To display information about current IPv6 Routing Information Protocol (RIP) processes, use the **show ipv6 rip** command in user EXEC or privileged EXEC mode.

```
show ipv6 rip [name] [vrf vrf-name][{database | next-hops}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>(Optional) Name of the RIP process. If the name is not entered, details of all configured RIP processes are displayed.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Displays information about the specified Virtual Routing and Forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>database</code></td>
<td>(Optional) Displays information about entries in the specified RIP IPv6 routing table.</td>
</tr>
<tr>
<td><code>next-hops</code></td>
<td>(Optional) Displays information about the next hop addresses for the specified RIP IPv6 process. If no RIP process name is specified, the next-hop addresses for all RIP IPv6 processes are displayed.</td>
</tr>
</tbody>
</table>

### Command Default

Information about all current IPv6 RIP processes is displayed.

### Command Modes

User EXEC (>)

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the **show ipv6 rip** command:

```
Device# show ipv6 rip

RIP process "one", port 521, multicast-group FF02::9, pid 55
  Administrative distance is 25. Maximum paths is 4
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
  Periodic updates 8883, trigger updates 2
  Interfaces:
    Ethernet2
Redistribution:
  RIP process "two", port 521, multicast-group FF02::9, pid 61
  Administrative distance is 120. Maximum paths is 4
  Updates every 30 seconds, expire after 180
  Holddown lasts 0 seconds, garbage collect after 120
  Split horizon is on; poison reverse is off
  Default routes are not generated
```
The following is sample output from the `show ipv6 rip database` command.

```
Device# show ipv6 rip one database
RIP process "one", local RIB
2001:72D:1000::/64, metric 2
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
2001:72D:2000::/64, metric 2, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
2001:72D:3000::/64, metric 2, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
  Ethernet1/2001:DB8:0:ABCD::1, expires in 120 secs
2001:72D:4000::/64, metric 16, expired, [advertise 119/hold 0]
  Ethernet2/2001:DB8:0:ABCD::1
3004::/64, metric 2 tag 2A, installed
  Ethernet2/2001:DB8:0:ABCD::1, expires in 168 secs
```
The table below describes the significant fields shown in the display.

**Table 81: show ipv6 rip database Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP process</td>
<td>The name of the RIP process.</td>
</tr>
<tr>
<td>2001:72D:1000::/64</td>
<td>The IPv6 route prefix.</td>
</tr>
<tr>
<td>metric</td>
<td>Metric for the route.</td>
</tr>
<tr>
<td>installed</td>
<td>Route is installed in the IPv6 routing table.</td>
</tr>
<tr>
<td>Ethernet2/2001:DB8:0:ABCD::1</td>
<td>Interface and LL next hop through which the IPv6 route was learned.</td>
</tr>
<tr>
<td>expires in</td>
<td>The interval (in seconds) before the route expires.</td>
</tr>
<tr>
<td>advertise</td>
<td>For an expired route, the value (in seconds) during which the route will be advertised as expired.</td>
</tr>
<tr>
<td>hold</td>
<td>The value (in seconds) of the hold-down timer.</td>
</tr>
<tr>
<td>tag</td>
<td>Route tag.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ipv6 rip next-hops` command:

Device# show ipv6 rip one next-hops

RIP process "one", Next Hops
FE80::210:7BFF:FEC2:ACCF/Ethernet4/2 [1 routes]
FE80::210:7BFF:FEC2:B286/Ethernet4/2 [2 routes]

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

**Table 82: show ipv6 rip next-hops Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP process</td>
<td>The name of the RIP process.</td>
</tr>
<tr>
<td>2001:DB8:0:1::/64/Ethernet4/2</td>
<td>The next-hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes or explicit next hops received in IPv6 RIP advertisements.</td>
</tr>
<tr>
<td>Note</td>
<td>An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.</td>
</tr>
<tr>
<td>[1 routes]</td>
<td>The number of routes in the IPv6 RIP routing table using the specified next hop.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ipv6 rip vrf` command:

Device# show ipv6 rip vrf red
RIP VRF "red", port 521, multicast-group 2001:DB8::/32, pid 295
Administrative distance is 120. Maximum paths is 16
Updates every 30 seconds, expire after 180
Hold down lasts 0 seconds, garbage collect after 120
Split horizon is on; poison reverse is off
Default routes are not generated
Periodic updates 99, trigger updates 3
Full Advertisement 0, Delayed Events 0
Interfaces:
  Ethernet0/1
  Loopback2
Redistribution:
  None

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

Table 83: show ipv6 rip vrf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP VRF</td>
<td>The name of the RIP VRF.</td>
</tr>
<tr>
<td>port</td>
<td>The port that the RIP process is using.</td>
</tr>
<tr>
<td>multicast-group</td>
<td>The IPv6 multicast group of which the RIP process is a member.</td>
</tr>
<tr>
<td>Administrative distance</td>
<td>Used to rank the preference of sources of routing information. Connected routes have an administrative distance of 1 and are preferred over the same route learned by a protocol with a larger administrative distance value.</td>
</tr>
<tr>
<td>Updates</td>
<td>The value (in seconds) of the update timer.</td>
</tr>
<tr>
<td>expires after</td>
<td>The interval (in seconds) in which updates expire.</td>
</tr>
<tr>
<td>Holddown</td>
<td>The value (in seconds) of the hold-down timer.</td>
</tr>
<tr>
<td>garbage collect</td>
<td>The value (in seconds) of the garbage-collect timer.</td>
</tr>
<tr>
<td>Split horizon</td>
<td>The split horizon state is either on or off.</td>
</tr>
<tr>
<td>poison reverse</td>
<td>The poison reverse state is either on or off.</td>
</tr>
<tr>
<td>Default routes</td>
<td>The origination of a default route into RIP. Default routes are either generated or not generated.</td>
</tr>
<tr>
<td>Periodic updates</td>
<td>The number of RIP update packets sent on an update timer.</td>
</tr>
<tr>
<td>trigger updates</td>
<td>The number of RIP update packets sent as triggered updates.</td>
</tr>
</tbody>
</table>

The following is sample output from `show ipv6 rip vrf next-hops` command:

Device# show ipv6 rip vrf blue next-hops

RIP VRF "blue", local RIB
AAAA::/64, metric 2, installed
Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00, expires in 177 secs
Table 84: show ipv6 rip vrf next-hops Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP VRF</td>
<td>The name of the RIP VRF.</td>
</tr>
<tr>
<td>metric</td>
<td>Metric for the route.</td>
</tr>
<tr>
<td>installed</td>
<td>Route is installed in the IPv6 routing table.</td>
</tr>
<tr>
<td>Ethernet0/0/FE80::A8BB:CCFF:FE00:7C00</td>
<td>The next hop address and interface through which it was learned. Next hops are either the addresses of IPv6 RIP neighbors from which we have learned routes, or explicit next hops received in IPv6 RIP advertisements.</td>
</tr>
</tbody>
</table>

Note: An IPv6 RIP neighbor may choose to advertise all its routes with an explicit next hop. In this case the address of the neighbor would not appear in the next hop display.

expires in
The interval (in seconds) before the route expires.

The following is sample output from **show ipv6 rip vrf database** command:

Device# show ipv6 rip vrf blue database

RIP VRF "blue", Next Hops
FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0 [1 paths]

Table 85: show ipv6 rip vrf database Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIP VRF</td>
<td>The name of the RIP VRF.</td>
</tr>
<tr>
<td>FE80::A8BB:CCFF:FE00:7C00/Ethernet0/0</td>
<td>Interface and LL next hop through which the IPv6 route was learned.</td>
</tr>
<tr>
<td>1 paths</td>
<td>Indicates the number of unique paths to this router that exist in the routing table.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ipv6 rip</td>
<td>Deletes routes from the IPv6 RIP routing table.</td>
</tr>
<tr>
<td>debug ipv6 rip</td>
<td>Displays the current contents of the IPv6 RIP routing table.</td>
</tr>
<tr>
<td>ipv6  rip  vrf-mode enable</td>
<td>Enables VRF-aware support for IPv6 RIP.</td>
</tr>
</tbody>
</table>
**show ipv6 route**

To display contents of the IPv6 routing table, use the `show ipv6 route` command in user EXEC or privileged EXEC mode.

```
show ipv6 route [ipv6-address | ipv6-prefix/prefix-length longer-prefixes] [protocol] [repair]
[updated boot-up] [day month] [time] interface type number nd nsf table table-id watch
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>(Optional) Displays routing information for a specific IPv6 address.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>(Optional) Displays routing information for a specific IPv6 network.</td>
</tr>
<tr>
<td>/prefix-length</td>
<td>(Optional) The length of the IPv6 prefix. A decimal value that indicates how</td>
</tr>
<tr>
<td></td>
<td>many of the high-order contiguous bits of the address comprise the prefix</td>
</tr>
<tr>
<td></td>
<td>(the network portion of the address). A slash mark must precede the decimal</td>
</tr>
<tr>
<td></td>
<td>value.</td>
</tr>
<tr>
<td>longer-prefixes</td>
<td>(Optional) Displays output for longer prefix entries.</td>
</tr>
<tr>
<td>protocol</td>
<td>(Optional) The name of a routing protocol or the keyword connected, local,</td>
</tr>
<tr>
<td></td>
<td>mobile, or static. If you specify a routing protocol, use one of the</td>
</tr>
<tr>
<td></td>
<td>following keywords: bgp, isis, eigrp, ospf, or rip.</td>
</tr>
<tr>
<td>repair</td>
<td>(Optional) Displays routes with repair paths.</td>
</tr>
<tr>
<td>updated</td>
<td>(Optional) Displays routes with time stamps.</td>
</tr>
<tr>
<td>boot-up</td>
<td>(Optional) Displays routing information since bootup.</td>
</tr>
<tr>
<td>day month</td>
<td>(Optional) Displays routes since the specified day and month.</td>
</tr>
<tr>
<td>time</td>
<td>(Optional) Displays routes since the specified time, in hh:mm format.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Displays information about the interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface number.</td>
</tr>
<tr>
<td>nd</td>
<td>(Optional) Displays only routes from the IPv6 Routing Information Base</td>
</tr>
<tr>
<td></td>
<td>(RIB) that are owned by Neighbor Discovery (ND).</td>
</tr>
<tr>
<td>nsf</td>
<td>(Optional) Displays routes in the nonstop forwarding (NSF) state.</td>
</tr>
<tr>
<td>repair</td>
<td>(Optional)</td>
</tr>
<tr>
<td>table table-id</td>
<td>(Optional) Displays IPv6 RIB table information for the specified table ID.</td>
</tr>
<tr>
<td></td>
<td>The table ID must be in hexadecimal format. The range is from 0 to 0xFFFFF</td>
</tr>
<tr>
<td>watch</td>
<td>(Optional) Displays information about route watchers.</td>
</tr>
</tbody>
</table>
**Command Default**

If none of the optional syntax elements is chosen, all IPv6 routing information for all active routing tables is displayed.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 route` command provides output similar to the `show ip route` command, except that the information is IPv6-specific.

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, the longest match lookup is performed from the routing table, and only route information for that address or network is displayed. When a routing protocol is specified, only routes for that protocol are displayed. When the `connected`, `local`, `mobile`, or `static` keyword is specified, only the specified type of route is displayed. When the `interface` keyword and `type` and `number` arguments are specified, only routes for the specified interface are displayed.

**Examples**

The following is sample output from the `show ipv6 route` command when no keywords or arguments are specified:

```
Device# show ipv6 route
IPv6 Routing Table - 9 entries
Codes:  C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA = IIS interarea
B 2001:DB8:4::2/48 [20/0]
   via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
L 2001:DB8:4::3/48 [0/0]
   via ::, Ethernet1/0
C 2001:DB8:4::4/48 [0/0]
   via ::, Ethernet1/0
LC 2001:DB8:4::5/48 [0/0]
   via ::, Loopback0
L 2001:DB8:4::6/48 [0/0]
   via ::, Serial6/0
C 2001:DB8:4::7/48 [0/0]
   via ::, Serial6/0
S 2001:DB8:4::8/48 [1/0]
   via 2001:DB8::1::1, Null
L FE80::/10 [0/0]
   via ::, Null0
L FF00::/8 [0/0]
   via ::, Null0
```

The table below describes the significant fields shown in the display.
### Table 86: show ipv6 route Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes:</td>
<td>Indicates the protocol that derived the route. Values are as follows:</td>
</tr>
<tr>
<td></td>
<td>• B—BGP derived</td>
</tr>
<tr>
<td></td>
<td>• C—Connected</td>
</tr>
<tr>
<td></td>
<td>• I1—ISIS L1—Integrated IS-IS Level 1 derived</td>
</tr>
<tr>
<td></td>
<td>• I2—ISIS L2—Integrated IS-IS Level 2 derived</td>
</tr>
<tr>
<td></td>
<td>• IA—ISIS interarea—Integrated IS-IS interarea derived</td>
</tr>
<tr>
<td></td>
<td>• L—Local</td>
</tr>
<tr>
<td></td>
<td>• R—RIP derived</td>
</tr>
<tr>
<td></td>
<td>• S—Static</td>
</tr>
<tr>
<td>2001:DB8:4::2/48</td>
<td>Indicates the IPv6 prefix of the remote network.</td>
</tr>
<tr>
<td>[20/0]</td>
<td>The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.</td>
</tr>
<tr>
<td>via FE80::A8BB:CCFF:FE02:8B00</td>
<td>Specifies the address of the next device to the remote network.</td>
</tr>
</tbody>
</table>

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, only route information for that address or network is displayed. The following is sample output from the `show ipv6 route` command when IPv6 prefix 2001:DB8::/35 is specified. The fields in the display are self-explanatory.

```
Device# show ipv6 route 2001:DB8::/35

IPv6 Routing Table - 261 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::/35 [20/3]
  via FE80:::60:5C59:9E00:16, Tunnel1
```

When you specify a protocol, only routes for that particular routing protocol are shown. The following is sample output from the `show ipv6 route bgp` command. The fields in the display are self-explanatory.

```
Device# show ipv6 route bgp

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
B 2001:DB8::4::4/64 [20/0]
  via FE80::A8BB:CCFF:FE02:8B00, Serial6/0
```

The following is sample output from the `show ipv6 route local` command. The fields in the display are self-explanatory.
Device# show ipv6 route local

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
L 2001:DB8::2/128 [0/0]
   via ::, Ethernet1/0
LC 2001:DB8::1/128 [0/0]
   via ::, Loopback0
L 2001:DB8::3/128 [0/0]
   via ::, Serial6/0
L FE80::/10 [0/0]
   via ::, Null0
L FF00::/8 [0/0]
   via ::, Null0

The following is sample output from the show ipv6 route command when the 6PE multipath feature is enabled. The fields in the display are self-explanatory.

Device# show ipv6 route

IPv6 Routing Table - default - 19 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
U - Per-user Static route
I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
B 2001:DB8::/64 [200/0]
   via ::FFFF:172.16.0.1
   via ::FFFF:172.30.30.1

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 route</td>
<td>Establishes a static IPv6 route.</td>
</tr>
<tr>
<td>show ipv6 interface</td>
<td>Displays IPv6 interface information.</td>
</tr>
<tr>
<td>show ipv6 route summary</td>
<td>Displays the current contents of the IPv6 routing table in summary format.</td>
</tr>
<tr>
<td>show ipv6 tunnel</td>
<td>Displays IPv6 tunnel information.</td>
</tr>
</tbody>
</table>
**show ipv6 routers**

To display IPv6 router advertisement (RA) information received from on-link devices, use the `show ipv6 routers` command in user EXEC or privileged EXEC mode.

```
show ipv6 routers [interface-type interface-number][conflicts][vrf vrf-name][detail]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type</code></td>
<td>(Optional) Specifies the Interface type.</td>
</tr>
<tr>
<td><code>interface-number</code></td>
<td>(Optional) Specifies the Interface number.</td>
</tr>
<tr>
<td><code>conflicts</code></td>
<td>(Optional) Displays RAs that differ from the RAs configured for a specified interface.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Provides detail about the eligibility of the neighbor for election as the default device.</td>
</tr>
</tbody>
</table>

### Command Default

When an interface is not specified, on-link RA information is displayed for all interface types. (The term *on-link* refers to a locally reachable address on the link.)

### Command Modes

- User EXEC (`>`)
- Privileged EXEC (`#`)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Devices that advertise parameters that differ from the RA parameters configured for the interface on which the RAs are received are marked as conflicting.

### Examples

The following is sample output from the `show ipv6 routers` command when entered without an IPv6 interface type and number:

```
Device# show ipv6 routers

Device FE80::83B3:60A4 on Tunnel5, last update 3 min
    Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
    Reachable time 0 msec, Retransmit time 0 msec
    Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
        Valid lifetime -1, preferred lifetime -1
Device FE80::290:27FF:FE8C:B709 on Tunnel157, last update 0 min
    Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
    Reachable time 0 msec, Retransmit time 0 msec
```

The following sample output shows a single neighboring device that is advertising a high default device preference and is indicating that it is functioning as a Mobile IPv6 home agent on this link.

```
Device# show ipv6 routers
```

---

**IP Addressing Services**

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following table describes the significant fields shown in the displays.

**Table 87: show ipv6 routers Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hops</td>
<td>The configured hop limit value for the RA.</td>
</tr>
<tr>
<td>Lifetime</td>
<td>The configured lifetime value for the RA. A value of 0 indicates that the device is not a default device. A value other than 0 indicates that the device is a default device.</td>
</tr>
<tr>
<td>AddrFlag</td>
<td>If the value is 0, the RA received from the device indicates that addresses are not configured using the stateful autoconfiguration mechanism. If the value is 1, the addresses are configured using this mechanism.</td>
</tr>
<tr>
<td>OtherFlag</td>
<td>If the value is 0, the RA received from the device indicates that information other than addresses is not obtained using the stateful autoconfiguration mechanism. If the value is 1, other information is obtained using this mechanism. (The value of OtherFlag can be 1 only if the value of AddrFlag is 1.)</td>
</tr>
<tr>
<td>MTU</td>
<td>The maximum transmission unit (MTU).</td>
</tr>
<tr>
<td>HomeAgentFlag=1</td>
<td>The value can be either 0 or 1. A value of 1 indicates that the device from which the RA was received is functioning as a mobile IPv6 home agent on this link, and a value of 0 indicates it is not functioning as a mobile IPv6 home agent on this link.</td>
</tr>
<tr>
<td>Preference=High</td>
<td>The DRP value, which can be high, medium, or low.</td>
</tr>
<tr>
<td>Retransmit time</td>
<td>The configured RetransTimer value. The time value to be used on this link for neighbor solicitation transmissions, which are used in address resolution and neighbor unreachability detection. A value of 0 means the time value is not specified by the advertising device.</td>
</tr>
<tr>
<td>Prefix</td>
<td>A prefix advertised by the device. Also indicates if on-link or autoconfig bits were set in the RA message.</td>
</tr>
<tr>
<td>Valid lifetime</td>
<td>The length of time (in seconds) relative to the time the advertisement is sent that the prefix is valid for the purpose of on-link determination. A value of -1 (all ones, 0xffffffff) represents infinity.</td>
</tr>
<tr>
<td>preferred lifetime</td>
<td>The length of time (in seconds) relative to the time the advertisements is sent that addresses generated from the prefix via address autoconfiguration remain valid. A value of -1 (all ones, 0xffffffff) represents infinity.</td>
</tr>
</tbody>
</table>

When the `interface-type` and `interface-number` arguments are specified, RA details about that specific interface are displayed. The following is sample output from the `show ipv6 routers` command when entered with an interface type and number:
Device# `show ipv6 routers tunnel 5`

Device FE80::83B3:60A4 on Tunnel5, last update 5 min
   Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
       Valid lifetime -1, preferred lifetime -1

Entering the `conflicts` keyword with the `show ipv6 routers` command displays information for devices that are advertising parameters different from the parameters configured for the interface on which the advertisements are being received, as the following sample output shows:

Device# `show ipv6 routers conflicts`

Device FE80::203:FDF:FE34:7039 on Ethernet1, last update 1 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2003::/64 onlink autoconfig
       Valid lifetime -1, preferred lifetime -1
Device FE80::201:42FF:FECA:A5C on Ethernet1, last update 0 min, CONFLICT
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
   Reachable time 0 msec, Retransmit time 0 msec
   Prefix 2001::/64 onlink autoconfig
       Valid lifetime -1, preferred lifetime -1

Use of the `detail` keyword provides information about the preference rank of the device, its eligibility for election as default device, and whether the device has been elected:

Device# `show ipv6 routers detail`

Device FE80::A8BB:CCFF:FE00:5B00 on Ethernet0/0, last update 0 min
   Rank 0x811 (elegible), Default Router
   Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0, MTU=1500
   HomeAgentFlag=0, Preference=Medium, trustlevel = 0
   Reachable time 0 (unspecified), Retransmit time 0 (unspecified)
   Prefix 2001::/64 onlink autoconfig
       Valid lifetime 2592000, preferred lifetime 604800
show ipv6 rpf

To check Reverse Path Forwarding (RPF) information for a given unicast host address and prefix, use the `show ipv6 rpf` command in user EXEC or privileged EXEC mode.

```
show ipv6 rpf {source-vrf [access-list] | vrf receiver-vrf[source-vrf [access-list] | select}}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-vrf</td>
<td>Name or address of the virtual routing and forwarding (VRF) on which lookups are to be performed.</td>
</tr>
<tr>
<td>receiver-vrf</td>
<td>Name or address of the VRF in which the lookups originate.</td>
</tr>
<tr>
<td>access-list</td>
<td>Name or address of access control list (ACL) to be applied to the group-based VRF selection policy.</td>
</tr>
<tr>
<td>vrf</td>
<td>Displays information about the VRF instance.</td>
</tr>
<tr>
<td>select</td>
<td>Displays group-to-VRF mapping information.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 rpf` command displays information about how IPv6 multicast routing performs Reverse Path Forwarding (RPF). Because the router can find RPF information from multiple routing tables (for example, unicast Routing Information Base [RIB], multiprotocol Border Gateway Protocol [BGP] routing table, or static mroutes), the `show ipv6 rpf` command to display the source from which the information is retrieved.

**Examples**

The following example displays RPF information for the unicast host with the IPv6 address of 2001::1:1:2:

```
Device# show ipv6 rpf 2001::1:1:2
RPF information for 2001::1:1:2
  RPF interface:Ethernet3/2
  RPF neighbor:FE80::40:1:3
  RPF route/mask:20::/64
  RPF type:Unicast
  RPF recursion count:0
  Metric preference:110
  Metric:30
```

The table below describes the significant fields shown in the display.
### Table 88: `show ipv6 rpf` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPF information for 2001::1:1:2</td>
<td>Source address that this information concerns.</td>
</tr>
<tr>
<td>RPF interface:Ethernet3/2</td>
<td>For the given source, the interface from which the router expects to get packets.</td>
</tr>
<tr>
<td>RPF neighbor:FE80::40:1:3</td>
<td>For the given source, the neighbor from which the router expects to get packets.</td>
</tr>
<tr>
<td>RPF route/mask:20::/64</td>
<td>Route number and mask that matched against this source.</td>
</tr>
<tr>
<td>RPF type:Unicast</td>
<td>Routing table from which this route was obtained, either unicast, multiprotocol BGP, or static mroutes.</td>
</tr>
<tr>
<td>RPF recursion count</td>
<td>Indicates the number of times the route is recursively resolved.</td>
</tr>
<tr>
<td>Metric preference:110</td>
<td>The preference value used for selecting the unicast routing metric to the Route Processor (RP) announced by the designated forwarder (DF).</td>
</tr>
<tr>
<td>Metric:30</td>
<td>Unicast routing metric to the RP announced by the DF.</td>
</tr>
</tbody>
</table>
show ipv6 source-guard policy

To display the IPv6 source-guard policy configuration, use the `show ipv6 source-guard policy` command in user EXEC or privileged EXEC mode.

```
show ipv6 source-guard policy [source-guard-policy]
```

**Syntax Description**

| **source-guard-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 Modes**

- User EXEC (`>`)
- Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 source-guard policy` command displays the IPv6 source-guard policy configuration, as well as all the interfaces on which the policy is applied. The command also displays IPv6 prefix guard information if the IPv6 prefix guard feature is enabled on the device.

**Examples**

```
Device# show ipv6 source-guard policy policy1

Policy policy1 configuration:
data-glean
prefix-guard
address-guard

Policy policy1 is applied on the following targets:
Target  Type  Policy  Feature  Target range
Et0/0   PORT  policy1  source-guard  vlan all
vlan 100  VLAN  policy1  source-guard  vlan all
```

**Related Commands**

<table>
<thead>
<tr>
<th><strong>Command</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 source-guard attach-policy</td>
<td>Applies IPv6 source guard on an interface.</td>
</tr>
<tr>
<td>ipv6 source-guard policy</td>
<td>Defines an IPv6 source-guard policy name and enters source-guard policy configuration mode.</td>
</tr>
</tbody>
</table>
show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the `show ipv6 spd` command in privileged EXEC mode.

```
show ipv6 spd
```

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

**Command Modes**
Privileged EXEC (#)

**Command History**
- **Release**
  - Cisco IOS XE Everest 16.5.1a
- **Modification**
  - This command was introduced.

**Usage Guidelines**
Use the `show ipv6 spd` command to display the SPD configuration, which may provide useful troubleshooting information.

**Examples**
The following is sample output from the `show ipv6 spd` command:

```
Device# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

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

**Table 89: show ipv6 spd Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current mode: normal</td>
<td>The current SPD state or mode.</td>
</tr>
<tr>
<td>Queue max threshold: 74</td>
<td>The process input queue maximum.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 spd queue max-threshold</td>
<td>Configures the maximum number of packets in the SPD process input queue.</td>
</tr>
</tbody>
</table>
show ipv6 static

To display the current contents of the IPv6 routing table, use the `show ipv6 static` command in user EXEC or privileged EXEC mode.

```
show ipv6 static [ {ipv6-address | ipv6-prefix/prefix-length} ] [ { interface type number | recursive } ] [ detail ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6-address</td>
<td>(Optional) Provides routing information for a specific IPv6 address. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>ipv6-prefix</td>
<td>(Optional) Provides routing information for a specific IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</td>
</tr>
<tr>
<td>/prefix-length</td>
<td>(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</td>
</tr>
<tr>
<td>interface</td>
<td>(Optional) Name of an interface.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional, but required if the <code>interface</code> keyword is used) Interface type. For a list of supported interface types, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional, but required if the <code>interface</code> keyword is used) Interface number. For specific numbering syntax for supported interface types, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>recursive</td>
<td>(Optional) Allows the display of recursive static routes only.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Specifies the following additional information:</td>
</tr>
<tr>
<td></td>
<td>• For valid recursive routes, the output path set and maximum resolution depth.</td>
</tr>
<tr>
<td></td>
<td>• For invalid recursive routes, the reason why the route is not valid.</td>
</tr>
<tr>
<td></td>
<td>• For invalid direct or fully specified routes, the reason why the route is not valid.</td>
</tr>
</tbody>
</table>

### Command Default

All IPv6 routing information for all active routing tables is displayed.

### Command Modes

User EXEC (`~`)

Privileged EXEC (`#`)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

The `show ipv6 static` command provides output similar to the `show ip route` command, except that it is IPv6-specific.

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, a longest match lookup is performed from the routing table and only route information for that address or network is displayed. Only the information matching the criteria specified in the command syntax is displayed. For example, when the `type number` arguments are specified, only the specified interface-specific routes are displayed.

Examples

show ipv6 static Command with No Options Specified in the Command Syntax: Example

When no options specified in the command, those routes installed in the IPv6 Routing Information Base (RIB) are marked with an asterisk, as shown in the following example:

```
Device# show ipv6 static
IPv6 Static routes
Code: * - installed in RIB
  * 3000::/16, interface Ethernet1/0, distance 1
  * 4000::/16, via nexthop 2001:1::1, distance 1
  5000::/16, interface Ethernet3/0, distance 1
  * 5555::/16, via nexthop 4000::1, distance 1
  5555::/16, via nexthop 9999::1, distance 1
  * 5555::/16, interface Ethernet2/0, distance 1
  * 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1
```

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

```
Table 90: show ipv6 static Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>via nexthop</td>
<td>Specifies the address of the next Device in the path to the remote network.</td>
</tr>
<tr>
<td>distance 1</td>
<td>Indicates the administrative distance to the specified route.</td>
</tr>
</tbody>
</table>
```

show ipv6 static Command with the IPv6 Address and Prefix: Example

When the `ipv6-address` or `ipv6-prefix/prefix-length` argument is specified, only information about static routes for that address or network is displayed. The following is sample output from the `show ipv6 route` command when entered with the IPv6 prefix `2001:200::/35`:

```
Device# show ipv6 static 2001:200::/35
IPv6 Static routes
Code: * - installed in RIB
  * 2001:200::/35, via nexthop 4000::1, distance 1
  2001:200::/35, via nexthop 9999::1, distance 1
  * 2001:200::/35, interface Ethernet2/0, distance 1
```
**show ipv6 static interface Command: Example**

When an interface is supplied, only those static routes with the specified interface as the outgoing interface are displayed. The `interface` keyword may be used with or without the IPv6 address and prefix specified in the command statement.

```
Device# show ipv6 static interface ethernet 3/0
```

IPv6 Static routes Code: * - installed in RIB 5000::/16, interface Ethernet3/0, distance 1

**show ipv6 static recursive Command: Example**

When the `recursive` keyword is specified, only recursive static routes are displayed:

```
Device# show ipv6 static recursive
```

IPv6 Static routes Code: * - installed in RIB * 4000::/16, via nexthop 2001:1::1, distance 1 * 5555::/16, via nexthop 4000::1, distance 1 5555::/16, via nexthop 9999::1, distance 1

**show ipv6 static detail Command: Example**

When the `detail` keyword is specified, the following additional information is displayed:

- For valid recursive routes, the output path set and maximum resolution depth.
- For invalid recursive routes, the reason why the route is not valid.
- For invalid direct or fully specified routes, the reason why the route is not valid.

```
Device# show ipv6 static detail
```

IPv6 Static routes
Code: * - installed in RIB
* 3000::/16, interface Ethernet1/0, distance 1
* 4000::/16, via nexthop 2001:1::1, distance 1
  Resolves to 1 paths (max depth 1)
  via Ethernet1/0
  5000::/16, interface Ethernet3/0, distance 1
  Interface is down
* 5555::/16, via nexthop 4000::1, distance 1
  Resolves to 1 paths (max depth 2)
  via Ethernet1/0
  5555::/16, via nexthop 9999::1, distance 1
  Route does not fully resolve
* 5555::/16, interface Ethernet2/0, distance 1
* 6000::/16, via nexthop 2007::1, interface Ethernet1/0, distance 1

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6 route</td>
<td>Establishes a static IPv6 route.</td>
</tr>
<tr>
<td>show ip route</td>
<td>Displays the current state of the routing table.</td>
</tr>
</tbody>
</table>
### Command Reference

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show ipv6 interface</code></td>
<td>Displays IPv6 interface information.</td>
</tr>
<tr>
<td><code>show ipv6 route summary</code></td>
<td>Displays the current contents of the IPv6 routing table in summary format.</td>
</tr>
<tr>
<td><code>show ipv6 tunnel</code></td>
<td>Displays IPv6 tunnel information.</td>
</tr>
</tbody>
</table>
show ipv6 traffic

To display statistics about IPv6 traffic, use the `show ipv6 traffic` command in user EXEC or privileged EXEC mode.

```
show ipv6 traffic [interface[interface  type number]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface</strong></td>
<td>(Optional) All interfaces. IPv6 forwarding statistics for all interfaces on which IPv6 forwarding statistics are being kept will be displayed.</td>
</tr>
<tr>
<td><strong>interface type number</strong></td>
<td>(Optional) Specified interface. Interface statistics that have occurred since the statistics were last cleared on the specific interface are displayed.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ipv6 traffic` command provides output similar to the `show ip traffic` command, except that it is IPv6-specific.

**Examples**

The following is sample output from the `show ipv6 traffic` command:

```
Device# show ipv6 traffic
IPv6 statistics:
Rcvd: 0 total, 0 local destination
  0 source-routed, 0 truncated
  0 format errors, 0 hop count exceeded
  0 bad header, 0 unknown option, 0 bad source
  0 unknown protocol, 0 not a device
  0 fragments, 0 total reassembled
  0 reassembly timeouts, 0 reassembly failures
  0 unicast RPF drop, 0 suppressed RPF drop
Sent: 0 generated, 0 forwarded
  0 fragmented into 0 fragments, 0 failed
  0 encapsulation failed, 0 no route, 0 too big
Mcast: 0 received, 0 sent
ICMP statistics:
Rcvd: 0 input, 0 checksum errors, 0 too short
  0 unknown info type, 0 unknown error type
  unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
  parameter: 0 error, 0 header, 0 option
  0 hopcount expired, 0 reassembly timeout,0 too big
  0 echo request, 0 echo reply
  0 group query, 0 group report, 0 group reduce
  0 device solicit, 0 device advert, 0 redirects
```

The following is sample output for the `show ipv6 interface` command without IPv6 CEF running:
Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
Description: sat-2900a f0/12
Global unicast address(es):
    7::7, subnet is 7::/32
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
Input features: RPF
Unicast RPF access-list MINI
Process Switching:
    0 verification drops
    0 suppressed verification drops
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds

The following is sample output for the show ipv6 interface command with IPv6 CEF running:

Device# show ipv6 interface ethernet 0/1/1
Ethernet0/1/1 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::203:FDFF:FE49:9
Description: sat-2900a f0/12
Global unicast address(es):
    7::7, subnet is 7::/32
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:7
    FF02::1:FF49:9
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
Input features: RPF
Unicast RPF access-list MINI
Process Switching:
    0 verification drops
    0 suppressed verification drops
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.

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

Table 91: show ipv6 traffic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-routed</td>
<td>Number of source-routed packets.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
truncated | Number of truncated packets.
format errors | Errors that can result from checks performed on header fields, the version number, and packet length.
not a device | Message sent when IPv6 unicast routing is not enabled.
0 unicast RPF drop, 0 suppressed RPF drop | Number of unicast and suppressed reverse path forwarding (RPF) drops.
failed | Number of failed fragment transmissions.
encapsulation failed | Failure that can result from an unresolved address or try-and-queue packet.
no route | Counted when the software discards a datagram it did not know how to route.
unreach | Unreachable messages received are as follows:
  - routing--Indicates no route to the destination.
  - admin--Indicates that communication with the destination is administratively prohibited.
  - neighbor--Indicates that the destination is beyond the scope of the source address. For example, the source may be a local site or the destination may not have a route back to the source.
  - address--Indicates that the address is unreachable.
  - port--Indicates that the port is unreachable.
Unicast RPF access-list MINI | Unicast RPF access-list in use.
Process Switching | Displays process RPF counts, such as verification and suppressed verification drops.
CEF Switching | Displays CEF switching counts, such as verification drops and suppressed verification drops.
show key chain

To display the keychain, use the **show key chain** command.

**show key chain**  *name-of-chain*

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name-of-chain</td>
<td>(Optional) Name of the key chain to display, as named in the key chain command.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key-string</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
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 | ip sla | brief | ipv6 route | brief | list | route | brief | resolution | ip | ipv6 | stub-object | brief | summary | timers]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>object-number</code></td>
<td>(Optional) Object number that represents the object to be tracked. The range is from 1 to 1000.</td>
</tr>
<tr>
<td><code>brief</code></td>
<td>(Optional) Displays a single line of information related to the preceding argument or keyword.</td>
</tr>
<tr>
<td><code>application</code></td>
<td>(Optional) Displays tracked application objects.</td>
</tr>
<tr>
<td><code>interface</code></td>
<td>(Optional) Displays tracked interface objects.</td>
</tr>
<tr>
<td><code>ip route</code></td>
<td>(Optional) Displays tracked IP route objects.</td>
</tr>
<tr>
<td><code>ip sla</code></td>
<td>(Optional) Displays tracked IP SLA objects.</td>
</tr>
<tr>
<td><code>ipv6 route</code></td>
<td>(Optional) Displays tracked IPv6 route objects.</td>
</tr>
<tr>
<td><code>list</code></td>
<td>(Optional) Displays the list of boolean objects.</td>
</tr>
<tr>
<td><code>resolution</code></td>
<td>(Optional) Displays resolution of tracked parameters.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays the summary of the specified object.</td>
</tr>
<tr>
<td><code>timers</code></td>
<td>(Optional) Displays polling interval timers.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.
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 92: show track Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Track</td>
<td>Object number that is being tracked.</td>
</tr>
<tr>
<td>Interface GigabitEthernet 1/0/1 ip routing</td>
<td>Interface type, interface number, and object that is being tracked.</td>
</tr>
<tr>
<td>IP routing is</td>
<td>State value of the object, displayed as Up or Down. If the object is down, the reason is displayed.</td>
</tr>
<tr>
<td>1 change, last change</td>
<td>Number of times that the state of a tracked object has changed and the time (in hh:mm:ss) since the last change.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show track resolution</td>
<td>Displays the resolution of tracked parameters.</td>
</tr>
<tr>
<td>track interface</td>
<td>Configures an interface to be tracked and enters tracking configuration mode.</td>
</tr>
<tr>
<td>track ip route</td>
<td>Tracks the state of an IP route and enters tracking configuration mode.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>object-number</td>
<td>Object number in the range from 1 to 1000 representing the interface to be tracked.</td>
</tr>
<tr>
<td>interface type number</td>
<td>Interface type and number to be tracked.</td>
</tr>
<tr>
<td>line-protocol</td>
<td>Tracks whether the interface is up.</td>
</tr>
<tr>
<td>ip routing</td>
<td>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.</td>
</tr>
<tr>
<td>ipv6 routing</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command Default**
The state of the interfaces is not tracked.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)# 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>glbp weighting</td>
<td>Specifies the initial weighting value of a GLBP gateway.</td>
</tr>
<tr>
<td>glbp weighting track</td>
<td>Specifies an object to be tracked that affects the weighting of a GLBP gateway.</td>
</tr>
</tbody>
</table>
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group-id</code></td>
<td>Virtual router group number. The range is from 1 to 255.</td>
</tr>
<tr>
<td><code>address-family</code></td>
<td>Specifies the address-family for this VRRP group.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Specifies IPv4 address.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Specifies IPv6 address.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced..</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>timers advertise</code></td>
<td>Sets the advertisement timer in milliseconds.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Text (up to 80 characters) that describes the purpose or use of the group.</td>
</tr>
</tbody>
</table>

**Command Default**

There is no description of the VRRP group.

**Command Modes**

VRRP configuration (config-if-vrrp)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>Creates a VRRPv3 group and enters VRRPv3 group configuration mode.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>delay minimum seconds</code></td>
<td>(Optional) Number of seconds that the device will delay before issuing an advertisement claiming master ownership. The default delay is 0 seconds.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is enabled.

**Command Modes**

VRRP configuration (config-if-vrrp)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>Creates a VRRPv3 group and enters VRRPv3 group configuration mode.</td>
</tr>
<tr>
<td>priority</td>
<td>Sets the priority level of the device within a VRRP group.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>level</code></td>
<td>Priority of the device within the VRRP group. The range is from 1 to 254. The default is 100.</td>
</tr>
</tbody>
</table>

**Command Default**

The priority level is set to the default value of 100.

**Command Modes**

VRRP configuration (config-if-vrrp)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrrp</code></td>
<td>Creates a VRRPv3 group and enters VRRPv3 group configuration mode.</td>
</tr>
<tr>
<td><code>vrrp preempt</code></td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>group</strong></td>
<td>Virtual router group number. The group number range is from 1 to 255.</td>
</tr>
<tr>
<td><strong>msec</strong></td>
<td>(Optional) Changes the unit of the advertisement time from seconds to milliseconds. Without this keyword, the advertisement interval is in seconds.</td>
</tr>
<tr>
<td><strong>interval</strong></td>
<td>Time interval between successive advertisements by the master virtual router. The unit of the interval is in seconds, unless the <code>msec</code> keyword is specified. The default is 1 second. The valid range is 1 to 255 seconds. When the <code>msec</code> keyword is specified, the valid range is 50 to 999 milliseconds.</td>
</tr>
</tbody>
</table>

### Command Default

The default interval of 1 second is configured.

### Command Modes

VRRP configuration (config-if-vrrp)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrrp</td>
<td>Creates a VRRPv3 group and enters VRRPv3 group configuration mode.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timers learn</td>
<td>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.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrrs-leader-name</code></td>
<td>Name of VRRS Tag to lead.</td>
</tr>
</tbody>
</table>

**Command Default**

A registered VRRS name is unavailable by default.

**Command Modes**

VRRP configuration (config-if-vrrp)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example specifies a leader's name to be registered with VRRS:

```
Device(config-if-vrrp)# vrrs leader leader-1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrrp</code></td>
<td>Creates a VRRP group and enters VRRP configuration mode.</td>
</tr>
</tbody>
</table>
PART V

IP Multicast Routing

• IP Multicast Routing Commands, on page 615
IP Multicast Routing Commands

- clear ip mfib counters, on page 617
- clear ip mroute, on page 618
- clear ip pim snooping vlan, on page 619
- ip igmp filter, on page 620
- ip igmp max-groups, on page 621
- ip igmp profile, on page 623
- ip igmp snooping, on page 624
- ip igmp snooping last-member-query-count, on page 625
- ip igmp snooping querier, on page 627
- ip igmp snooping report-suppression, on page 629
- ip igmp snooping vlan mrouter, on page 630
- ip igmp snooping vlan static, on page 631
- ip multicast auto-enable, on page 632
- ip multicast-routing, on page 633
- ip pim accept-register, on page 634
- ip pim bidir-enable, on page 635
- ip pim bsr-candidate, on page 636
- ip pim rp-address, on page 638
- ip pim rp-candidate, on page 640
- ip pim send-rp-announce, on page 641
- ip pim snooping, on page 643
- ip pim snooping dr-flood, on page 644
- ip pim snooping vlan, on page 645
- ip pim spt-threshold, on page 646
- match message-type, on page 647
- match service-type, on page 648
- match service-instance, on page 649
- mrinfo, on page 650
- service-policy-query, on page 652
- service-policy, on page 653
- show ip igmp filter, on page 654
- show ip igmp profile, on page 655
- show ip igmp snooping, on page 656
• show ip igmp snooping groups, on page 658
• show ip igmp snooping mrouter, on page 660
• show ip igmp snooping querier, on page 661
• show ip pim autorp, on page 663
• show ip pim bsr-router, on page 664
• show ip pim bsr, on page 665
• show ip pim interface df, on page 666
• show ip pim rp, on page 668
• show ip pim snooping, on page 670
• show ip pim tunnel, on page 673
• show platform software fed switch ip multicast groups, on page 675
• show platform software fed switch ip multicast, on page 676
• show platform software fed switch ip multicast df, on page 679
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.
- **group-address** (Optional) Limits the active MFIB traffic counters to the indicated group address.
- **hostname** (Optional) Limits the active MFIB traffic counters to the indicated host name.
- **source-address** (Optional) Limits the active MFIB traffic counters to the indicated source address.

**Command Default**

None

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
clear ip mroute [vrf vrf-name] { * | ip-address | group-address } [hostname | source-address]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
- ***** Specifies all Multicast routes.
- **ip-address** Multicast routes for the IP address.
- **group-address** Multicast routes for the group address.
- **hostname** (Optional) Multicast routes for the host name.
- **source-address** (Optional) Multicast routes for the source address.

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
clear ip pim snooping vlan

To delete the Protocol Independent Multicast (PIM) snooping entries on a specific VLAN, use the `clear ip pim snooping vlan` command in user EXEC or privileged EXEC mode.

```
clear ip pim snooping vlan vlan-id [{neighbor | statistics | mroute} [{source-ipgroup-ip}]])
```

**Syntax Description**

- `vlan vlan-id` - VLAN ID. Valid values are from 1—4094.
- `neighbor` - Deletes all the neighbors.
- `statistics` - Deletes information about the VLAN statistics.
- `mroute group-addr src-addr` - Deletes the mroute entries in the specified group and the source IP address.

**Command Default**
This command has no default settings.

**Command Modes**
User EXEC
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to clear the IP PIM-snooping entries on a specific VLAN:

```
Router# clear ip pim snooping vlan 1001
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip pim snooping</code></td>
<td>Enables PIM snooping globally.</td>
</tr>
<tr>
<td><code>show ip pim snooping</code></td>
<td>Displays information about IP PIM snooping.</td>
</tr>
</tbody>
</table>
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**
- `profile number` – 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max number</code></td>
<td>Maximum number of IGMP groups that an interface can join. The range is 0—4294967294. The default is no limit.</td>
</tr>
<tr>
<td><code>action deny</code></td>
<td>Drops the next IGMP join report when the maximum number of entries is in the IGMP snooping forwarding table. This is the default action.</td>
</tr>
<tr>
<td><code>action replace</code></td>
<td>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.</td>
</tr>
</tbody>
</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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-id</code></td>
<td>(Optional) Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.</td>
</tr>
</tbody>
</table>

**Command Default**

IGMP snooping is globally enabled on the device.

IGMP snooping is enabled on VLAN interfaces.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 vlan-id** (Optional) Sets the count value on a specific VLAN ID. The range is from 1—1001. Do not enter leading zeroes.
- **count** 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 (count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 milliseconds and a count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.
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 vlan-id` (Optional) Enables IGMP snooping and the IGMP querier function on the specified VLAN. Ranges are 1–1001 and 1006–4094.

- `address ip-address` (Optional) Specifies a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier.

- `max-response-time response-time` (Optional) Sets the maximum time to wait for an IGMP querier report. The range is 1–25 seconds.

- `query-interval interval-count` (Optional) Sets the interval between IGMP queriers. The range is 1–18000 seconds.

- `tcn query {count count | interval interval}` (Optional) Sets parameters related to Topology Change Notifications (TCNs).

- `count count` Sets the number of TCN queries to be executed during the TCN interval time. The range is 1–10.

- `interval interval` Sets the TCN query interval time. The range is 1–255.

- `timer expiry expiry-time` (Optional) Sets the length of time until the IGMP querier expires. The range is 60–300 seconds.

- `version version` (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Command Default**
By default, there are no multicast router ports.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>Enables IGMP snooping on the specified VLAN. Ranges are 1—1001 and 1006—4094.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>Adds a Layer 2 port as a member of a multicast group with the specified group IP address.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>Specifies the interface of the member port. The <code>interface-id</code> has these options:</td>
</tr>
<tr>
<td></td>
<td>• <code>fastethernet interface number</code>—A Fast Ethernet IEEE 802.3 interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>gigabitethernet interface number</code>—A Gigabit Ethernet IEEE 802.3z interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>tengigabitethernet interface number</code>—A 10-Gigabit Ethernet IEEE 802.3z interface.</td>
</tr>
<tr>
<td></td>
<td>• <code>port-channel interface number</code>—A channel interface. The range is 0—128.</td>
</tr>
</tbody>
</table>

### Command Default

By default, no ports are statically configured as members of a multicast group.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
None

**Example**
The following example shows how to enable AAA on IP multicast:

```
Device(config)# ip multicast auto-enable
```
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]
oip multicast-routing  [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRF) instance specified for the vrf-name argument.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>instance specified for the vrf-name argument.</td>
</tr>
</tbody>
</table>

**Command Default**

IP multicast routing is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When IP multicast routing is disabled, the Cisco IOS XE 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:

```
Device> enable
Device# configure terminal
Device(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Device(config)# ip multicast-routing vrf vrf1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim</td>
<td>Enables PIM on an interface.</td>
</tr>
</tbody>
</table>
ip pim accept-register

To configure a candidate rendezvous point (RP) switch to filter Protocol Independent Multicast (PIM) register messages, use the `ip pim accept-register` command in global configuration mode. To disable this function, use the `no` form of this command.

```
ip pim [vrf vrf-name] accept-register {list access-list}
no ip pim [vrf vrf-name] accept-register
```

**Syntax Description**

- **vrf vrf-name** (Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the `vrf-name` argument.

- **list access-list** Specifies the `access-list` argument as a number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied. The range is 100—199 and the expanded range is 2000—2699. An IP-named access list can also be used.

**Command Default**

No PIM register filters are configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 bidir-enable

To enable bidirectional Protocol Independent Multicast (bidirectional PIM), use the `ip pim bidir-enable` command in global configuration mode. To disable bidirectional PIM, use the `no` form of this command.

```
ip pim bidir-enable
no ip pim bidir-enable
```

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Default**
The command is enabled.

**Command Modes**
Global configuration (config)

**Usage Guidelines**
When bidirectional PIM is disabled, the router will behave similarly to a router without bidirectional PIM support. The following conditions will apply:

- PIM hello messages sent by the router will not contain the bidirectional mode option.
- The router will not send designated forwarder (DF) election messages and will ignore DF election messages it receives.
- The `ip pim rp-address`, `ip pim send-rp-announce`, and `ip pim rp-candidate` global configuration commands will be treated as follows:
  - If these commands are configured when bidirectional PIM is disabled, bidirectional mode will not be a configuration option.
  - If these commands are configured with the bidirectional mode option when bidirectional PIM is enabled and then bidirectional PIM is disabled, these commands will be removed from the command-line interface (CLI). In this situation, these commands must be configured again with the bidirectional mode option when bidirectional PIM is reenabled.
- The `df` keyword for the `show ip pim interface` user EXEC or privileged EXEC command and `debug ip pim` privileged EXEC command is not supported.

The following example shows how to enable bidirectional PIM:

```
Device# enable
Device# configure terminal
Device(config)# ip pim bidir-enable
```
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 vrf-name` (Optional) Configures the Device to be a candidate BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the `vrf-name` argument.

- `interface-id` ID of the interface on 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.

- `hash-mask-length` (Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.

- `priority` (Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred.

**Command Default**

The Device is not configured to announce itself as a candidate BSR.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

```
ip pim [vrf vrf-name] rp-address rp-address [access-list] [override] [bidir]
no ip pim [vrf vrf-name] rp-address rp-address [access-list] [override] [bidir]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the vrf-name argument.</td>
</tr>
<tr>
<td><strong>rp-address rp-address</strong></td>
<td>IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.</td>
</tr>
<tr>
<td><strong>access-list</strong></td>
<td>(Optional) Number or name of a standard access list that defines the multicast groups to be statically mapped to the RP. <strong>Note</strong> If no access list is defined, the RP will map to all multicast groups</td>
</tr>
<tr>
<td><strong>override</strong></td>
<td>(Optional) Specifies that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. <strong>Note</strong> If the <strong>override</strong> keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.</td>
</tr>
<tr>
<td><strong>bidir</strong></td>
<td>(Optional) Specifies that the static group-to-RP mapping be applied to a bidirectional PIM RP. If the command is configured without the <strong>bidir</strong> keyword, the groups will operate in sparse mode. <strong>Note</strong> The <strong>bidir</strong> keyword is available as an optional keyword only if bidirectional PIM has been enabled using the <strong>ip pim bidir-enable</strong> command.</td>
</tr>
</tbody>
</table>
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Command Default

No PIM static group-to-RP mappings are configured.

Command Modes

Global configuration (config)

Usage Guidelines

Under PIM, multicast groups in sparse mode (PIM-SM) or bidirectional mode (bidirectional PIM) use RPs to connect sources and receivers. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The Cisco IOS software learns the mode and RP addresses of multicast groups through the following three mechanisms: static group-to-RP mapping configurations, Auto-RP, and bootstrap router (BSR).

Use the `ip pim rp-address` command to statically define the RP address for PIM-SM or bidirectional PIM groups (an `ip pim rp-address` command configuration is referred to as a static group-to-RP mapping).

You can configure a single RP for more than one group using an access list. If no access list is specified, the static RP will map to all multicast groups.

You can configure multiple RPs, but only one RP per group range.

If multiple `ip pim rp-address` commands are configured, the following rules apply:

- Highest RP IP address selected regardless of reachability: If a multicast group is matched by the access list of more than one configured `ip pim rp-address` command, then the RP for the group is determined by the RP with the highest RP address configured.

- One RP address per command: If multiple `ip pim rp-address` commands are configured, each static group-to-RP mapping must be configured with a unique RP address (if not, it will be overwritten). This restriction also means that only one RP address can be used to provide RP functions for either sparse mode or bidirectional mode groups. If you want to configure static group-to-RP mappings for both bidirectional and sparse mode, the RP addresses must be unique for each mode.

- One access list per command: If multiple `ip pim rp-address` commands are configured, only one access list can be configured per static group-to-RP mapping. An access list cannot be reused with other static group-to-RP mappings configured on a router.

If dynamic and static group-to-RP mappings are used together, the following rule applies to a multicast group: Dynamic group-to-RP mappings take precedence over static group-to-RP mappings--unless the `override` keyword is used.

The following example shows how to set the bidirectional PIM RP address to 172.16.0.2 for the multicast range 239/8:

```
Device(config)# access list 10 239.0.0.0 0.255.255.255
Device(config)# ip pim rp-address 172.16.0.2 10 bidir
```
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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Configures the switch to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the <strong>vrf-name</strong> argument.</td>
</tr>
<tr>
<td>interface-id</td>
<td>ID of the interface whose associated IP address is advertised as a candidate RP address. Valid interfaces include physical ports, port channels, and VLANs.</td>
</tr>
<tr>
<td>group-list access-list-number</td>
<td>(Optional) Specifies the standard IP access list number that defines the group prefixes that are advertised in association with the RP address.</td>
</tr>
</tbody>
</table>

**Command Default**
The Device is not configured to announce itself to the BSR as a PIMv2 C-RP.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```
no ip pim [vrf vrf-name] send-rp-announce interface-id scope ttl-value [group-list access-list-number] [interval seconds] [bidir]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Uses Auto-RP to configure groups for which the device will act as a rendezvous point (RP) for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td><code>interface-id</code></td>
<td>Enter the interface ID of the interface that identifies the RP address. Valid interfaces include physical ports, port channels, and VLANs.</td>
</tr>
<tr>
<td><code>scope ttl-value</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>group-list access-list-number</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>interval seconds</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>bidir</code></td>
<td>(Optional) Indicates that the multicast groups specified by the access-list argument are to operate in bidirectional mode. If the command is configured without this keyword, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).</td>
</tr>
</tbody>
</table>

**Command Default**

Auto-RP is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was modified. The <code>bidir</code> keyword was added.</td>
</tr>
</tbody>
</table>

**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.
Use this command with the `bidir` keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-RP mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-RP mappings, use the `bidir` keyword with the `ip pim rp-candidate` command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the `bidir` keyword with the `ip pim rp-address` command.

**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:

```bash
Device(config)# ip pim send-rp-announce GigabitEthernet1/0/1 scope 31 group-list 5 interval 120
```
### ip pim snooping

To enable Protocol Independent Multicast (PIM) snooping globally, use the `ip pim snooping` command in global configuration mode. To disable PIM snooping globally, use the `no` form of this command.

```
ip pim snooping
no ip pim snooping
```

#### Syntax Description

This command has no arguments or keywords.

#### Command Default

PIM snooping is not enabled.

#### Command Modes

Global configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

When you disable PIM snooping globally, PIM snooping is disabled on all the VLANs.

#### Examples

The following example shows how to enable PIM snooping globally:

```
ip pim snooping
```

The following example shows how to disable PIM snooping globally:

```
no ip pim snooping
```

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip pim snooping</td>
<td>Deletes PIM snooping on an interface.</td>
</tr>
<tr>
<td>show ip pim snooping</td>
<td>Displays information about IP PIM snooping.</td>
</tr>
</tbody>
</table>
ip pim snooping dr-flood

To enable flooding of packets to the designated router, use the `ip pim snooping dr-flood` command in global configuration mode. To disable the flooding of packets to the designated router, use the `no` form of this command.

```
ip pim snooping dr-flood
no ip pim snooping dr-flood
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The flooding of packets to the designated router is enabled by default.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

Enter the `no ip pim snooping dr-flood` command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

**Examples**

The following example shows how to enable flooding of packets to the designated router:

```
   ip pim snooping dr-flood
```

The following example shows how to disable flooding of packets to the designated router:

```
   no ip pim snooping dr-flood
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip pim snooping</td>
<td>Deletes PIM snooping on an interface.</td>
</tr>
<tr>
<td>show ip pim snooping</td>
<td>Displays information about IP PIM snooping.</td>
</tr>
</tbody>
</table>
ip pim snooping vlan

To enable Protocol Independent Multicast (PIM) snooping on an interface, use the **ip pim snooping vlan** command in global configuration mode. To disable PIM snooping on an interface, use the **no** form of this command.

```
ip pim snooping vlan vlan-id
no ip pim snooping vlan vlan-id
```

**Syntax Description**

| VLAN ID value. The range is 1—1001. Do not enter leading zeroes. |

**Command Default**
PIM snooping is disabled on an interface.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

This command automatically configures the VLAN if it is not already configured. The configuration is saved in NVRAM.

**Examples**

This example shows how to enable PIM snooping on a VLAN interface:

```
Router(config)# ip pim snooping vlan 2
```

This example shows how to disable PIM snooping on a VLAN interface:

```
Router(config)# no ip pim snooping vlan 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip pim snooping</td>
<td>Deletes PIM snooping on an interface.</td>
</tr>
<tr>
<td>ip pim snooping</td>
<td>Enables PIM snooping globally.</td>
</tr>
<tr>
<td>show ip pim snooping</td>
<td>Displays information about IP PIM snooping.</td>
</tr>
</tbody>
</table>
ip pim spt-threshold

To specify the threshold that must be reached before moving to shortest-path tree (spt), use the `ip pim spt-threshold` command in global configuration mode. To remove the threshold, use the `no` form of this command.

```
ip pim {kbps | infinity} [group-list access-list]
no ip pim {kbps | infinity} [group-list access-list]
```

**Syntax Description**

- **kbps**
  - 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

`line`  
Regular expression to match the service type in packets.

### Command Default

None

### Command Modes

Service list configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

- `line`  
  Regular expression to match the service instance in packets.

**Command Default**

None

**Command Modes**

Service list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

- **vrf route-name** (Optional) Specifies the VPN routing or forwarding instance.
- **hostname | address** (Optional) Domain Name System (DNS) name or IP address of the multicast router or multilayer switch to query. If omitted, the switch queries itself.
- **interface-id** (Optional) Interface ID.

**Command Default**
The command is disabled.

**Command Modes**
User EXEC
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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]
```
The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol-capable
- A: Auto RP capable
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**

- `service-list-query-name` (Optional) Service-list query periodicity.

**Command Default**

Disabled.

**Command Modes**

mDNS configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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-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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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-pol1 IN
```
show ip igmp filter

To display Internet Group Management Protocol (IGMP) filter information, use the `show ip igmp filter` command in privileged EXEC mode.

```
show ip igmp [vrf vrf-name] filter
```

**Syntax Description**

- `vrf vrf-name` (Optional) Supports the multicast VPN routing and forwarding (VRF) instance.

**Command Default**

IGMP filters are enabled by default.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 vlan-id** (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094.
- **detail** (Optional) Displays operational state information.

**Command Default**

None

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 vlan-id` (Optional) Specifies a VLAN; the range is 1 to 1001 and 1006 to 4094. Use this option to display the multicast table for a specified multicast VLAN or specific multicast information.

- `count` (Optional) Displays the total number of entries for the specified command options instead of the actual entries.

- `ip_address` (Optional) Characteristics of the multicast group with the specified group IP address.

**Command Modes**

- Privileged EXEC
- User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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   v2        Gi1/0/11
1        224.1.4.5   igmp   v2        Gi1/0/11
2        224.0.1.40  igmp   v2        Gi1/0/15
104      224.1.4.2   igmp   v2        Gi2/0/1, Gi2/0/2
104      224.1.4.3   igmp   v2        Gi2/0/1, Gi2/0/2
```

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, Gi2/0/2
```
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>104</td>
<td>224.1.4.2</td>
<td>igmp</td>
<td>v2</td>
<td>Gi2/0/1, Gi1/0/15</td>
</tr>
</tbody>
</table>
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 vlan-id**  (Optional) Specifies a VLAN; Ranges are from 1—1001 and 1006—4094.

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- VLAN IDs 1002—1005 are reserved for Token Ring and FDDI VLANs, and cannot be used in IGMP snooping.
- When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.
- Expressions are case sensitive, for example, if you enter | exclude output, the lines that contain "output" do not appear, but the lines that contain "Output" appear.

**Example**

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 vlan-id` (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

**Expression Reference**

- `| exclude output`: Lines that contain "output" do not appear, but the lines that contain "Output" appear.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 interface df**

To display information about the elected designated forwarder (DF) for each rendezvous point (RP) on an interface configured for Bidirectional Protocol Independent Multicast (PIM), use the `show ip pim interface df` command in user EXEC or privileged EXEC mode.

```
show ip pim [vrf vrf-name] interface [interface-type|interface-name] df [rp-address]
```

- **vrf vrf-name** (Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
- **interface [interface-type|interface-name]** Specifies the interface type or the interface number.
- **rp-address** (Optional) Specifies the RP IP address.

**Command History**

- Release: Cisco IOS XE Gibraltar 16.12.1
- Modification: This command was introduced.

**Command Default**

If no interface is specified, all interfaces are displayed.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

The following is sample output from the `show ip pim interface df` command:

```
Device# show ip pim interface df
Interface  show ip pim interface df
Ethernet3/3  DF Winner  Metric  Uptime
  10.10.0.2  10.4.0.2  0       00:03:49
  10.10.0.3  10.4.0.3  0       00:01:49
  10.10.0.5  10.4.0.4  409600  00:01:49
Ethernet3/4  10.10.0.2  10.5.0.2  0  00:03:49
  10.10.0.3  10.5.0.2  409600  00:02:32
  10.10.0.5  10.5.0.2  435200  00:02:16
Loopback0   10.10.0.2  10.10.0.2  0       00:03:49
  10.10.0.3  10.10.0.2  409600  00:02:32
  10.10.0.5  10.10.0.2  435200  00:02:16
```

The following is sample output from the `show ip pim interface df` command when an interface is specified:

```
Device# show ip pim interface Ethernet3/3 df 10.10.0.3
Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP 10.10.0.3
State       Non-DF
Offer count is 0
Current DF ip address   10.4.0.3
DF winner up time       00:02:33
Last winner metric preference 0
Last winner metric      0
```

The following table gives the output field descriptions for the `show ip pim interface df` command:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies the interface type or the interface number.</td>
</tr>
<tr>
<td>RP</td>
<td>Specifies the RP IP address.</td>
</tr>
<tr>
<td>DF Winner</td>
<td>Specifies the elected designated forwarder (DF) address.</td>
</tr>
<tr>
<td>Metric</td>
<td>Specifies the preference metric.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Specifies the up time.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RP</td>
<td>IP address of the RP.</td>
</tr>
<tr>
<td>DF Winner</td>
<td>IP address of the elected DF.</td>
</tr>
<tr>
<td>Metric</td>
<td>Unicast routing metric to the RP announced by the DF.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Length of time the RP has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the specified interface is an elected DF.</td>
</tr>
<tr>
<td>Offer count is</td>
<td>Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.</td>
</tr>
<tr>
<td>Current DF IP address</td>
<td>IP address of the current DF.</td>
</tr>
<tr>
<td>DF winner uptime</td>
<td>Length of time the current DF has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.</td>
</tr>
<tr>
<td>Last winner metric preference</td>
<td>The preference value used for selecting the unicast routing metric to the RP announced by the DF.</td>
</tr>
<tr>
<td>Last winner metric</td>
<td>Unicast routing metric to the RP announced by the DF.</td>
</tr>
</tbody>
</table>
show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the show ip pim rp command in user EXEC or privileged EXEC mode.

```
show ip pim [vrf vrf-name] rp [mapping [ elected | in-use ] | metric] [rp-address]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
- `mapping [ elected | in-use ]` (Optional) Displays all group-to-RP mappings of which the router is aware. (either configured or learned from Auto-RP)
  - `elected` - Displays elected Auto RPs.
  - `in-use` - Displays learned RPs in-use.
- `metric` (Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
- `rp-address` (Optional) Specifies the RP IP address.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Default**

If no RP is specified, all active RPs are displayed.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Usage Guidelines**

The Protocol Independent Multicast (PIM) version known for an RP influences the type of PIM register messages (Version 1 or Version 2) that the router sends when acting as the designated router (DR) for an active source. If an RP is statically configured, the PIM version of the RP is not set and the router, if required to send register packets, tries to send PIM Version 2 register packets. If sending PIM Version 2 packets fails, the router sends PIM Version 1 register packets.

The version of the RP displayed in the `show ip pim rp` command output can change according to the operations of the router. When the group is created, the version shown is for the RP in the RP mapping cache. Later, the version displayed by this command may change. If this router is acting as a DR for an active source, the router sends PIM register messages. The PIM register messages are answered by the RP with PIM register stop messages. The router learns from these PIM register stop messages the actual PIM version of the RP. Once the actual PIM version of the RP is learned, this command displays only this version. If the router is not acting as a DR for active sources on this group, then the version shown for the RP of the group does not change. In this case, the PIM version of the RP is irrelevant to the router because the version of the RP influences only the PIM register messages that this router must send.
When you enter the `show ip pim rp mapping` command, the version of the RP displayed in the output is determined only by the method through which an RP is learned. If the RP is learned from Auto-RP then the RP displayed is either “v1” or “v2, v1.” If the RP is learned from a static RP definition, the RP version is undetermined and no RP version is displayed in the output. If the RP is learned from the BSR, the RP version displayed is “v2.”

The following is sample output from the `show ip pim rp` command:

```
Device# show ip pim rp
Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

The following is sample output from the `show ip pim rp` command when the `mapping` keyword is specified:

```
Device# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent
Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
    Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
    Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
    Uptime:00:00:52, expires:00:00:37
Group(s) (-230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
    Uptime:00:00:52, expires:00:00:37
```

The following is sample output from the `show ip pim rp` command when the `metric` keyword is specified:

```
Device# show ip pim rp metric
RP Address   Metric Pref Metric Flags RPF Type Interface
10.10.0.2   0     0     L    unicast Loopback0
10.10.0.3   90    409600 L    unicast Ethernet3/3
10.10.0.5   90    435200 L    unicast Ethernet3/3
```
show ip pim snooping

To display the information about IP PIM snooping, use the `show ip pim snooping` command in user EXEC or privileged EXEC mode.

**Global Status**

```
show ip pim snooping
```

**VLAN Status**

```
show ip pim snooping vlan vlan-id [{neighbor | statistics | mroute [{source-ip |group-ip}]]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan-id</code></td>
<td>Displays information for a specific VLAN; Valid values are from 1—4094.</td>
</tr>
<tr>
<td><code>neighbor</code></td>
<td>(Optional) Displays information about the neighbor database.</td>
</tr>
<tr>
<td><code>statistics</code></td>
<td>(Optional) Displays information about the VLAN statistics.</td>
</tr>
<tr>
<td><code>mroute</code></td>
<td>(Optional) Displays information about the mroute database.</td>
</tr>
<tr>
<td><code>source-ip</code></td>
<td>(Optional) Source IP address.</td>
</tr>
<tr>
<td><code>group-ip</code></td>
<td>(Optional) Group IP address.</td>
</tr>
</tbody>
</table>

### Command Default

This command has no default settings.

### Command Modes

User EXEC Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to display information about the global status:

```
Router# show ip pim snooping

Global runtime mode: Enabled
Global admin mode : Enabled
DR Flooding status : Disabled
SGR-Prune Suppression: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 1001

This example shows how to display information about a specific VLAN:

```
Router# show ip pim snooping vlan 1001

4 neighbors (0 DR priority incapable, 4 Bi-dir incapable)
5000 mroutes, 0 mac entries
DR is 10.10.10.4
RP DF Set:
QinQ snooping : Disabled
This example shows how to display information about the neighbor database for a specific VLAN:

Router# `show ip pim snooping vlan 1001 neighbor`

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Mac address</th>
<th>Port</th>
<th>Uptime/Expires</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.2</td>
<td>000a.f330.344a</td>
<td>Po128</td>
<td>02:52:27/00:01:41</td>
<td></td>
</tr>
<tr>
<td>10.10.10.1</td>
<td>000a.f330.334a</td>
<td>Hu1/0/7</td>
<td>04:54:14/00:01:38</td>
<td></td>
</tr>
<tr>
<td>10.10.10.4</td>
<td>000a.f330.3c00</td>
<td>Hu1/0/1</td>
<td>04:53:45/00:01:34</td>
<td>DR</td>
</tr>
</tbody>
</table>

This example shows how to display the detailed statistics for a specific VLAN:

Router# `show ip pim snooping vlan 1001 statistics`

PIMv2 statistics:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>56785</td>
</tr>
<tr>
<td>Process Enqueue</td>
<td>56785</td>
</tr>
<tr>
<td>Process PIMv2 input queue current outstanding</td>
<td>0</td>
</tr>
<tr>
<td>Process PIMv2 input queue max size reached</td>
<td>110</td>
</tr>
<tr>
<td>Error - Global Process State not RUNNING</td>
<td>0</td>
</tr>
<tr>
<td>Error - Process Enqueue</td>
<td>0</td>
</tr>
<tr>
<td>Error - Drops</td>
<td>0</td>
</tr>
<tr>
<td>Error - Bad packet floods</td>
<td>0</td>
</tr>
<tr>
<td>Error - IP header generic error</td>
<td>0</td>
</tr>
<tr>
<td>Error - IP header payload len too long</td>
<td>0</td>
</tr>
<tr>
<td>Error - IP header payload len too short</td>
<td>0</td>
</tr>
<tr>
<td>Error - IP header checksum</td>
<td>0</td>
</tr>
<tr>
<td>Error - IP header dest ip not 224.0.0.13</td>
<td>0</td>
</tr>
<tr>
<td>Error - PIM header payload len too short</td>
<td>0</td>
</tr>
<tr>
<td>Error - PIM header checksum</td>
<td>0</td>
</tr>
<tr>
<td>Error - PIM header checksum in Registers</td>
<td>0</td>
</tr>
<tr>
<td>Error - PIM header version not 2</td>
<td>0</td>
</tr>
</tbody>
</table>

This example shows how to display information about the mroute database for all the mrouters in a specific VLAN:

Router# `show ip pim snooping vlan 10 mroute`

Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
SGR-P - (S,G,R) Prune

VLAN 1001: 5000 mroutes

(*, 225.0.1.0), 00:14:54/00:02:59
Downstream ports: Po128
Upstream ports: Hu1/0/7
Outgoing ports: Hu1/0/7 Po128

(10.10.10.105, 225.0.1.0), 00:14:54/00:02:59
10.10.10.130->10.10.10.105, 00:14:54/00:02:59, SGR-P
Downstream ports:
Upstream ports: Hu1/0/7
Outgoing ports:

(*, 225.0.5.1), 00:14:53/00:02:57
10.10.10.105->10.10.10.10, 00:14:53/00:02:57, J
Downstream ports: Po128
Upstream ports: Hu1/0/7
Outgoing ports:

(11.11.11.10, 225.0.5.0), 00:14:53/00:02:57
10.10.10.105->10.10.10.130, 00:14:53/00:02:57, SGR-P
This example shows how to display information about the PIM mroute for a specific source address:

```
Router# show ip pim snooping vlan 10 mroute 172.16.100.100
(*, 172.16.100.100), 00:16:36/00:02:36
  10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
  Downstream ports: 3/12
  Upstream ports: 3/13
  Outgoing ports: 3/12 3/13
```

This example shows how to display information about the PIM mroute for a specific source and group address:

```
Router# show ip pim snooping vlan 10 mroute 192.168.0.0 172.16.10.10
(192.168.0.0, 172.16.10.10), 00:03:04/00:00:25
  10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
  Downstream ports: 3/12
  Upstream ports: 3/13
  Outgoing ports: 3/12 3/13
```

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

### Table 93: show ip pim snooping Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downstream ports</td>
<td>Ports on which PIM joins were received.</td>
</tr>
<tr>
<td>Upstream ports</td>
<td>Ports towards RP and source.</td>
</tr>
<tr>
<td>Outgoing ports</td>
<td>List of all upstream and downstream ports for the multicast flow.</td>
</tr>
</tbody>
</table>

```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip pim snooping vlan</td>
<td>Deletes PIM snooping on an interface.</td>
</tr>
<tr>
<td>ip pim snooping</td>
<td>Enables PIM snooping globally.</td>
</tr>
<tr>
<td>ip pim snooping vlan</td>
<td>Enables PIM snooping on an interface.</td>
</tr>
</tbody>
</table>
```
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a virtual routing and forwarding (VRF) configuration.</td>
</tr>
<tr>
<td>Tunnel interface-number</td>
<td>(Optional) Specifies the tunnel interface number.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Provides additional information, such as the MAC encapsulation header and platform-specific information.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 platform software fed switch ip multicast groups

To display platform-dependent IP multicast groups information, use the `show platform software fed switch ip multicast groups` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} ip multicast groups [vrf-id vrf-id | vrf-name vrf-name] [group-address [source source-address] [detail] [count] [summary]
```

**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.

- **vrf vrf-id**: (Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) ID.

- **vrf vrf-name**: (Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) name.

- **group-address**: (Optional) Specifies the IP Multicast Group Address.

- **source source-address**: (Optional) Specifies the IP Multicast Source Address.

- **detail**: (Optional) Specifies the IP Multicast group detail.

- **count**: (Optional) Specifies the IP Multicast group count.

- **summary**: (Optional) Specifies the Multicast group summary.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**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 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 {switch-number | active | standby}`: The device for which you want to display information.
  - `switch-number`: 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**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: 0x00000001f6 flags: C
No RFF 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 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 0x0 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

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show platform software fed switch ip multicast

<output truncated>
**show platform software fed switch ip multicast df**

To display information about platform-dependent IP multicast designated forwards (DF), use the `show platform software fed switch ip multicast df` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} ip multicast df [vrf-id vrf-id | vrf-name vrf-name] [[df-index]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>switch</strong> `{switch_num</td>
<td>active</td>
</tr>
<tr>
<td>- <strong>switch_num</strong></td>
<td>Enter the switch ID. Displays information for the specified switch.</td>
</tr>
<tr>
<td>- <strong>active</strong></td>
<td>Displays information for the active switch.</td>
</tr>
<tr>
<td>- <strong>standby</strong></td>
<td>Displays information for the standby switch, if available.</td>
</tr>
<tr>
<td><strong>vrf-id vrf-id</strong></td>
<td>(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) ID.</td>
</tr>
<tr>
<td><strong>vrf vrf-name</strong></td>
<td>(Optional) Specifies the multicast Virtual Routing and Forwarding (VRF) name.</td>
</tr>
<tr>
<td><strong>df-index</strong></td>
<td>(Optional) Specifies the DF index.</td>
</tr>
</tbody>
</table>

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

The following is sample output from the `show platform software fed switch ip multicast df` command:

```
Device# show platform software fed switch active ip multicast df
VRF-ID  DF-Index  Ref-Count  DF Set
-------------------------------------
 2       1          1  Vlan254
         1          1  Vlan186
         1          1  Vlan305
         1          1  Vlan135
         1          1  Tunnel4
         1          1  Null0
```

---

**IP Multicast Routing**

---
show platform software fed switch ip multicast df
PART VI

Layer 2/3

• Layer 2/3 Commands, on page 683
Layer 2/3 Commands

- avb, on page 685
- avb vlan, on page 686
- channel-group, on page 687
- channel-protocol, on page 690
- clear lacp, on page 691
- clear pagp, on page 692
- clear spanning-tree counters, on page 693
- clear spanning-tree detected-protocols, on page 694
- debug etherchannel, on page 695
- debug lacp, on page 696
- debug pagp, on page 697
- debug platform pm, on page 698
- debug platform udld, on page 699
- debug spanning-tree, on page 700
- interface port-channel, on page 702
- lacp max-bundle, on page 704
- lacp port-priority, on page 705
- lacp rate, on page 706
- lacp system-priority, on page 707
- no ptp enable, on page 708
- pagp learn-method, on page 709
- pagp port-priority, on page 711
- policy-map, on page 712
- port-channel, on page 714
- port-channel auto, on page 715
- port-channel load-balance, on page 716
- port-channel load-balance extended, on page 719
- port-channel min-links, on page 720
- ptp priority1 value, on page 721
- ptp priority2 value, on page 722
- ptp profile dot1as, on page 723
- mvrp vlan creation, on page 724
- mvrp registration, on page 725
• mvrp timer, on page 727
• rep admin vlan, on page 729
• rep block port, on page 730
• rep isl-age-timer, on page 732
• rep isl-retries, on page 733
• rep preempt delay, on page 734
• rep preempt segment, on page 735
• rep segment, on page 736
• rep stcn, on page 738
• show avb domain, on page 739
• show avb streams, on page 741
• show etherchannel, on page 742
• show interfaces rep detail, on page 745
• show lacp, on page 746
• show mstp port bandwidth, on page 750
• show mstp streams, on page 752
• show pagp, on page 754
• show platform etherchannel, on page 756
• show platform hardware fed active vlan ingress, on page 757
• show platform pm, on page 758
• show platform software fed switch ptp, on page 759
• show ptp brief, on page 761
• show ptp clock, on page 762
• show ptp parent, on page 763
• show ptp port, on page 764
• show rep topology, on page 765
• show udld, on page 767
• show vlan dot1q tag native, on page 771
• switchport, on page 772
• switchport access vlan, on page 773
• switchport mode, on page 774
• switchport nonegotiate, on page 776
• switchport trunk, on page 777
• switchport voice vlan, on page 780
• udld, on page 783
• udld fast-hello, on page 785
• udld port, on page 786
• udld reset, on page 788
• vtp mode, on page 789
avb

To enable AVB, use `avb` command in global configuration or interface configuration mode. To disable AVB on the switch, use the `no` form of the command.

```
  avb
  no avb
```

**Command Modes**

Global configuration (config)

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `avb` command in global configuration mode to enable AVB on the device.

Use the `avb` command in interface configuration mode to configure the interfaces, along the connectivity path, for AVB devices as dot1q trunk ports.

**Example**

This example shows how to enable AVB in global configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# avb
```

This example shows how to enable AVB in interface configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# interface te1/1/1
Device(config-if)# switchport mode trunk
Device(config-if)# exit
Device(config)# vlan 2
Device(config)# avb vlan 10
Device(config-vlan)# avb
```
avb vlan

To set a specified VLAN as the default AVB VLAN, use the `avb vlan` command in global configuration mode.

```
avb vlan  vlan-id
```

**Syntax Description**

- `vlan-id` The range for `vlan-id` varies from 2 to 4094.

**Command Default**

VLAN 2 is the default AVB VLAN.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command when you need to set the default AVB VLAN other than VLAN 2.

**Example**

This example shows how set a specified VLAN as the default AVB VLAN:

```
Device> enable
Device# configure terminal
Device(config)# interface te1/1/1
Device(config-if)# switchport mode trunk
Device(config-if)# exit
Device(config)# vlan 2
Device(config)# avb vlan 10
```
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.

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

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel-group-number</td>
<td>Channel group number. The range is 1 to 128.</td>
</tr>
<tr>
<td>mode</td>
<td>Specifies the EtherChannel mode.</td>
</tr>
<tr>
<td>active</td>
<td>Unconditionally enables Link Aggregation Control Protocol (LACP).</td>
</tr>
<tr>
<td>auto</td>
<td>Enables the Port Aggregation Protocol (PAgP) only if a PAgP device is detected.</td>
</tr>
<tr>
<td>non-silent</td>
<td>(Optional) Configures the interface for nonsilent operation when connected to a partner that is PAgP-capable. Use in PAgP mode with the <code>auto</code> or <code>desirable</code> keyword when traffic is expected from the other device.</td>
</tr>
<tr>
<td>desirable</td>
<td>Unconditionally enables PAgP.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the on mode.</td>
</tr>
<tr>
<td>passive</td>
<td>Enables LACP only if a LACP device is detected.</td>
</tr>
</tbody>
</table>

Command Default

No channel groups are assigned.

No mode is configured.

Command Modes

Interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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.

Although it is not necessary to disable the IP address that is assigned to a physical port that is part of a channel group, we strongly recommend that you do so.

You create Layer 3 port channels by using the interface port-channel command followed by the no switchport interface configuration command. Manually configure the port-channel logical interface before putting the interface into the channel group.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode.

Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When auto is enabled, silent operation is the default.

Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. An EtherChannel is formed with another port group that is in the desirable or auto mode. When desirable is enabled, silent operation is the default.

If you do not specify non-silent with the auto or desirable mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and rarely, if ever, sends packets. An example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In on mode, a usable EtherChannel exists only when both connected port groups are in the on mode.

Use care when using the on mode. This is a manual configuration, and ports on both ends of the EtherChannel must have the same configuration. If the group is misconfigured, packet loss or spanning-tree loops can occur.

Passive mode places a port into a negotiating state in which the port responds to received LACP packets but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch or on different switches in the stack (but not in a cross-stack configuration). Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

If you set the protocol by using the channel-protocol interface configuration command, the setting is not overridden by the channel-group interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x authentication on an EtherChannel port, an error message appears, and IEEE 802.1x authentication is not enabled.

Do not configure a secure port as part of an EtherChannel or configure an EtherChannel port as a secure port.
For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

Caution

Do not enable Layer 3 addresses on the physical EtherChannel ports. Do not assign bridge groups on the physical EtherChannel ports because it creates loops.

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

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 switch 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 switch stack. It uses LACP passive mode and assigns two ports on stack member 2 and one port on stack member 3 as static-access ports in VLAN 10 to channel 5:

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` command in interface configuration mode.

You must use the `channel-group` command in interface configuration mode 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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# channel-protocol lACP
```

You can verify your settings by entering the `show etherchannel [channel-group-number] protocol` command in privileged EXEC mode.
clear lacp

To clear Link Aggregation Control Protocol (LACP) channel-group counters, use the `clear lacp` command in privileged EXEC mode.

```
clear lacp [channel-group-number] counters
```

**Syntax Description**

- `channel-group-number` (Optional) Channel group number. The range is 1 to 128.
- `counters` Clears traffic counters.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# clear lacp counters
```

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

```
Device> enable
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` command in privileged EXEC mode.
clear pagp

To clear the Port Aggregation Protocol (PAgP) channel-group information, use the `clear pagp` command in privileged EXEC mode.

```
clear pagp [channel-group-number] counters
```

**Syntax Description**
- `channel-group-number` (Optional) Channel group number. The range is 1 to 128.
- `counters` Clears traffic counters.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# clear pagp counters
```

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

```
Device> enable
Device# clear pagp 10 counters
```

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

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>(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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-id</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Privileged EXEC</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If the `interface-id` value is not specified, spanning-tree counters are cleared for all interfaces.

This example shows how to clear spanning-tree counters for all interfaces:

```
Device> enable
Device# clear spanning-tree counters
```
clear spanning-tree detected-protocols

To restart the protocol migration process and force renegotiation with neighboring devices on the interface, use the `clear spanning-tree detected-protocols` command in privileged EXEC mode.

```
clear spanning-tree detected-protocols [interface interface-id]
```

**Syntax Description**

- `interface interface-id` (Optional) Restarts the protocol migration process on the specified interface. Valid interfaces include physical ports, VLANs, and port channels.
  
  The VLAN range is 1 to 4094.

**Command Modes**

- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
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.

```
debugetherchannel [{all | detail | error | event | idb }]
nodebugetherchannel [{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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

Although the **linecard** keyword is displayed in the command-line help, it is not supported.

This example shows how to display all EtherChannel debug messages:

```
Device> enable
Device# debug etherchannel all
```

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

```
Device> enable
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.

ddebug 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undebug etherchannel` command is the same as the `no debug etherchannel` command.

This example shows how to display all LACP debug messages:

```plaintext
Device> enable
Device# debug LACP all
```

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

```plaintext
Device> enable
Device# debug LACP event
```
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.

```
depagp  [[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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undepagp` command is the same as the `no debug pagp` command.

This example shows how to display all PAgP debug messages:

```
Device> enable
Device# debug pagp all
```

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

```
Device> enable
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.

```
display platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status | platform | pm-vectors | detail | ses | vlans}
no display platform pm {all | counters | errdisable | fec | if-numbers | l2-control | link-status | platform | pm-vectors | detail | ses | vlans}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Displays all port manager debug messages.</td>
</tr>
<tr>
<td><code>counters</code></td>
<td>Displays counters for remote procedure call (RPC) debug messages.</td>
</tr>
<tr>
<td><code>errdisable</code></td>
<td>Displays error-disabled-related events debug messages.</td>
</tr>
<tr>
<td><code>fec</code></td>
<td>Displays forwarding equivalence class (FEC) platform-related events debug messages.</td>
</tr>
<tr>
<td><code>if-numbers</code></td>
<td>Displays interface-number translation event debug messages.</td>
</tr>
<tr>
<td><code>l2-control</code></td>
<td>Displays Layer 2 control infra debug messages.</td>
</tr>
<tr>
<td><code>link-status</code></td>
<td>Displays interface link-detection event debug messages.</td>
</tr>
<tr>
<td><code>platform</code></td>
<td>Displays port manager function event debug messages.</td>
</tr>
<tr>
<td><code>pm-vectors</code></td>
<td>Displays port manager vector-related event debug messages.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays vector-function details.</td>
</tr>
<tr>
<td><code>ses</code></td>
<td>Displays service expansion shelf (SES) related event debug messages.</td>
</tr>
<tr>
<td><code>vlans</code></td>
<td>Displays VLAN creation and deletion event debug messages.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undebug platform pm` command is the same as the `no debug platform pm` command.

This example shows how to display debug messages related to the creation and deletion of VLANs:

```
Device> enable
Device# debug platform pm vlans
```
debug platform udld

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

```
deploy platform udld [{error | event}] [switch switch-number]
no deploy platform udld [{error | event}] [switch switch-number]
```

**Syntax Description**

- **error** (Optional) Displays error condition debug messages.
- **event** (Optional) Displays UDLD-related platform event debug messages.
- **switch**
  - **switch-number** (Optional) Displays UDLD debug messages for the specified stack member.

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undeploy platform udld` command is the same as the `no deploy platform udld` command.

When you enable debugging on a switch stack, it is enabled only on the active switch. To enable debugging on a stack member, you can start a session from the active switch by using the `session switch-number` command in privileged EXEC mode. 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.

```plaintext
display spanning-tree { all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast }
no display spanning-tree { all | backbonefast | bpdu | bpdu-opt | config | etherchannel | events | exceptions | general | mstp | pvst+ | root | snmp | synchronization | switch | uplinkfast }
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all spanning-tree debug messages.</td>
</tr>
<tr>
<td>backbonefast</td>
<td>Displays BackboneFast-event debug messages.</td>
</tr>
<tr>
<td>bpdu</td>
<td>Displays spanning-tree bridge protocol data unit (BPDU) debug messages.</td>
</tr>
<tr>
<td>bpdu-opt</td>
<td>Displays optimized BPDU handling debug messages.</td>
</tr>
<tr>
<td>config</td>
<td>Displays spanning-tree configuration change debug messages.</td>
</tr>
<tr>
<td>etherchannel</td>
<td>Displays EtherChannel-support debug messages.</td>
</tr>
<tr>
<td>events</td>
<td>Displays spanning-tree topology event debug messages.</td>
</tr>
<tr>
<td>exceptions</td>
<td>Displays spanning-tree exception debug messages.</td>
</tr>
<tr>
<td>general</td>
<td>Displays general spanning-tree activity debug messages.</td>
</tr>
<tr>
<td>ha</td>
<td>Displays high-availability spanning-tree debug messages.</td>
</tr>
<tr>
<td>mstp</td>
<td>Debugs Multiple Spanning Tree Protocol (MSTP) events.</td>
</tr>
<tr>
<td>pvst+</td>
<td>Displays per-VLAN spanning-tree plus (PVST+) event debug messages.</td>
</tr>
<tr>
<td>root</td>
<td>Displays spanning-tree root-event debug messages.</td>
</tr>
<tr>
<td>snmp</td>
<td>Displays spanning-tree Simple Network Management Protocol (SNMP) handling debug messages.</td>
</tr>
<tr>
<td>switch</td>
<td>Displays switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various device platforms.</td>
</tr>
<tr>
<td>synchronization</td>
<td>Displays the spanning-tree synchronization event debug messages.</td>
</tr>
<tr>
<td>uplinkfast</td>
<td>Displays UplinkFast-event debug messages.</td>
</tr>
</tbody>
</table>
Command Default

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `undebug spanning-tree` command is the same as the `no debug spanning-tree` command.

When you enable debugging on a stack, it is enabled only on the active switch. To enable debugging on the standby switch, start a session from the active switch by using the `session switch-number` command in privileged EXEC mode. Enter the `debug` command at the command-line prompt of the standby switch.

To enable debugging on the standby switch without first starting a session on the active switch, use the `remote command switch-number LINE` command in privileged EXEC mode.

This example shows how to display all spanning-tree debug messages:

```
Device> enable
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**

<table>
<thead>
<tr>
<th>port-channel-number</th>
<th>Channel group number. The range is 1 to 128.</th>
</tr>
</thead>
</table>

**Command Default**

No port channel logical interfaces are defined.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` command in interface configuration mode, 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.

You create Layer 3 port channels by using the `interface port-channel` command followed by the `no switchport` command in interface configuration mode. You should manually configure the port-channel logical interface before putting the interface into the channel group.

Only one port channel in a channel group is allowed.

---

**Caution**

When using a port-channel interface as a routed port, do not assign Layer 3 addresses on the physical ports that are assigned to the channel group.

---

**Caution**

Do not assign bridge groups on the physical ports in a channel group used as a Layer 3 port channel interface because it creates loops. You must also disable spanning tree.

---

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> enable
Device# configure terminal
Device(config)# interface port-channel 5
```

You can verify your setting by entering either the `show running-config` in privileged EXEC mode or the `show etherchannel channel-group-number detail` command in privileged EXEC mode.
**Iacp max-bundle**

To define the maximum number of active LACP ports allowed in a port channel, use the `iacp max-bundle` command in interface configuration mode. To return to the default setting, use the `no` form of this command.

```
iacp max-bundle max_bundle_number
no iacp max-bundle
```

**Syntax Description**

- `max_bundle_number` The maximum number of active LACP ports in the port channel. The range is 1 to 8. The default is 8.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 `iacp max-bundle` command must specify a number greater than the number specified by the `port-channel min-links` command.

Use the `show etherchannel summary` command in privileged EXEC mode 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> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# iacp 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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>priority</code></td>
<td>Port priority for LACP. The range is 1 to 65535.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is 32768.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `lACP port-priority` command in interface configuration mode 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.

The LACP port priorities are only effective if the ports are on the device that controls the LACP link. See the `lACP system-priority` command in global configuration mode for determining which device controls the link.

Use the `show lACP internal` command in privileged EXEC mode 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> enable
Device# configure terminal
Device(config)# 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` command in privileged EXEC mode.
lacp rate

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the \texttt{lacp rate} command in interface configuration mode. To return to the default settings, use the \texttt{no} form of this command

\begin{verbatim}
lacp rate [normal | fast]
no lacp rate
\end{verbatim}

\textbf{Syntax Description}

- \texttt{normal} Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled.
- \texttt{fast} Specifies that LACP control packets are ingressed at the fast rate, once every 1 second.

\textbf{Command Default}

The default ingress rate for control packets is 30 seconds after the link is bundled.

\textbf{Command Modes}

Interface configuration

\textbf{Command History}

\begin{tabular}{|l|l|}
\hline
Release & Modification \\
\hline
Cisco IOS XE Everest 16.5.1a & This command was introduced. \\
\hline
\end{tabular}

\textbf{Usage Guidelines}

Use this command to modify the duration of LACP timeout. The LACP timeout value on Cisco switch is three times the LACP rate that is configured on the interface. Using the \texttt{lacp rate} command, you can select the LACP timeout value for a switch to be either 90 seconds or 3 seconds.

This command is supported only on LACP-enabled interfaces.

This example shows how to specify the fast (1 second) ingress rate on interface GigabitEthernet 0/0:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitEthernet 0/0
Device(config-if)# lacp rate fast
```
**lACP system-priority**

To configure the system priority for the Link Aggregation Control Protocol (LACP), use the `lACP system-priority` command in global configuration mode on the device. To return to the default setting, use the `no` form of this command.

```
lACP system-priority priority
no lACP system-priority
```

**Syntax Description**

- `priority` System priority for LACP. The range is 1 to 65535.

**Command Default**

The default is 32768.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` command in privileged EXEC mode 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> enable
Device# configure terminal
Device(config)# lACP system-priority 20000
```

You can verify your settings by entering the `show lACP sys-id` command in privileged EXEC mode.
no ptp enable

To disable PTP on an interface, use the no ptp enable command in interface configuration mode.
To re-enable PTP on the same interface, use the ptp enable command in interface configuration mode.

Command Default
PTP is enabled on all the ports, by default.

Command Modes
Interface configuration (config-if)

Command History

Release     Modification
-----------  --------------------
Cisco IOS XE Fuji 16.8.1a  This command was introduced.

Usage Guidelines
PTP is enabled on all the ports, by default.

Example
This example shows how to disable PTP on an interface:

```
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# no ptp enable
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptp priority1 value</td>
<td>Specifies the priority 1 number to use for this clock</td>
</tr>
<tr>
<td>ptp priority2 value</td>
<td>Specifies the priority 2 number to use for this clock</td>
</tr>
<tr>
<td>ptp profile dot1as</td>
<td>Enables Generalized Precision Time Protocol (gPTP) globally.</td>
</tr>
</tbody>
</table>
pagp learn-method

To learn the source address of incoming packets received from an EtherChannel port, use the pagp learn-method command in interface configuration mode. To return to the default setting, use the no form of this command.

```
pagp learn-method {aggregation-port | physical-port}
no pagp learn-method
```

**Syntax Description**

- `aggregation-port`: Specifies address learning on the logical port channel. The device sends packets to the source using any port in the EtherChannel. This setting is the default. With aggregation-port learning, it is not important on which physical port the packet arrives.

- `physical-port`: Specifies address learning on the physical port within the EtherChannel. The device sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address.

**Command Default**
The default is aggregation-port (logical port channel).

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` commands in interface configuration mode 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` command in interface configuration mode. 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` command in global configuration mode. Use the `pagp learn-method` command in interface configuration mode 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> enable
Device# configure terminal
Device(config)# interface port-channel 2
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> enable
Device# configure terminal
```
Device(config)# interface port-channel 2
Device(config-if)# pagp learn-method aggregation-port

You can verify your settings by entering either the **show running-config** command in privileged EXEC mode or the **show pagp channel-group-number internal** command in privileged EXEC mode.
pagp port-priority

To select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent, use the `pagp port-priority` command in interface configuration mode. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. To return to the default setting, use the `no` form of this command.

```
pagp port-priority priority
no pagp port-priority
```

**Syntax Description**

`priority` Priority number. The range is from 0 to 255.

**Command Default**
The default is 128.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` commands in interface configuration mode 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` command in interface configuration mode. 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` command in global configuration mode. Use the `pagp learn-method` command in interface configuration mode only in this situation.

This example shows how to set the port priority to 200:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# pagp port-priority 200
```

You can verify your setting by entering the `show running-config` command in privileged EXEC mode or the `show pagp channel-group-number internal` command in privileged EXEC mode.
policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the `policy-map` command in global configuration mode. To delete a policy map, use the `no` form of this command.

```plaintext
policy-map [ type { access-control | control subscriber | packet-service | performance-monitor } ] policy-map name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>(Optional) Specifies the policy-map type.</td>
</tr>
<tr>
<td>access-control</td>
<td>(Optional) Enables the access-control specific policy map.</td>
</tr>
<tr>
<td>control subscriber</td>
<td>(Optional) Enables subscriber control policy domain.</td>
</tr>
<tr>
<td>packet-service</td>
<td>(Optional) Enables packet service policy map.</td>
</tr>
<tr>
<td>performance-monitor</td>
<td>(Optional) Enables policy map for the performance monitoring feature.</td>
</tr>
<tr>
<td>policy-map name</td>
<td>Specifies the policy map.</td>
</tr>
</tbody>
</table>

**Command Default**

The policy map is not configured.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration (config)

**Usage Guidelines**

Use the `policy-map` command to specify the name of the policy map to create (add or modify) before you configure policies for classes whose match criteria are defined in a class map with the `class-map` and `match` commands.

**Note**

You can configure class policies in a policy map only if the classes have match criteria defined for them.

**Note**

Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies.

A single policy map can be attached concurrently to more than one interface. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by the multiple policies. In such cases, if the policy map is already attached to other interfaces, the map is removed.

**Example:**

The following is sample output from the `policy-map` command:
Device# policy-map AVB-Output-Child-Policy

policy-map AVB-Output-Child-Policy
class VOIP-PRIORITY-QUEUE
  bandwidth remaining percent 30
  queue-buffers ratio 10
class MULTIMEDIA-CONFERENCING-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF41 percent 80
  queue-limit dscp AF31 percent 80
  queue-limit dscp AF42 percent 90
  queue-limit dscp AF32 percent 90
  queue-buffers ratio 10
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF21 percent 80
  queue-limit dscp AF22 percent 90
  queue-buffers ratio 10
class BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 15
  queue-limit dscp AF11 percent 80
  queue-limit dscp AF12 percent 90
  queue-limit dscp CS1 percent 80
  queue-buffers ratio 15
class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
**port-channel**

To convert the auto created EtherChannel into a manual channel and adding configuration on the EtherChannel, use the **port-channel** command in privileged EXEC mode.

```
port-channel  {channel-group-number  persistent | persistent }
```

**Syntax Description**

- **channel-group-number**  Channel group number. The range is 1 to 128.
- **persistent**  Converts the auto created EtherChannel into a manual channel and allows you to add configuration on the EtherChannel.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the **show etherchannel summary** command in privileged EXEC mode to display the EtherChannel information.

**Examples**

This example shows how to convert the auto created EtherChannel into a manual channel:

```
Device> enable
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
```

**Command Default**
By default, the auto-LAG feature is disabled globally and is enabled on all port interfaces.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
You can use the **show etherchannel auto** command in privileged EXEC mode to verify if the EtherChannel was created automatically.

**Examples**
This example shows how to enable the auto-LAG feature on the switch:

```
Device> enable
Device# configure terminal
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.

```
```

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-ip</td>
<td>Specifies load distribution based on the destination host IP address.</td>
</tr>
<tr>
<td>dst-mac</td>
<td>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.</td>
</tr>
<tr>
<td>dst-mixed-ip-port</td>
<td>Specifies load distribution based on the destination IPv4 or IPv6 address and the TCP/UDP (Layer 4) port number.</td>
</tr>
<tr>
<td>dst-port</td>
<td>Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>extended</td>
<td>Sets extended load balance methods among the ports in the EtherChannel. See the <code>port-channel load-balance extended</code> command.</td>
</tr>
<tr>
<td>src-dst-ip</td>
<td>Specifies load distribution based on the source and destination host IP address.</td>
</tr>
<tr>
<td>src-dst-mac</td>
<td>Specifies load distribution based on the source and destination host MAC address.</td>
</tr>
<tr>
<td>src-dst-mixed-ip-port</td>
<td>Specifies load distribution based on the source and destination host IP address and TCP/UDP (layer 4) port number.</td>
</tr>
<tr>
<td>src-dst-port</td>
<td>Specifies load distribution based on the source and destination TCP/UDP (Layer 4) port number.</td>
</tr>
<tr>
<td>src-ip</td>
<td>Specifies load distribution based on the source host IP address.</td>
</tr>
<tr>
<td>src-mac</td>
<td>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.</td>
</tr>
<tr>
<td>src-mixed-ip-port</td>
<td>Specifies load distribution based on the source host IP address and TCP/UDP (Layer 4) port number.</td>
</tr>
<tr>
<td>src-port</td>
<td>Specifies load distribution based on the TCP/UDP (Layer 4) port number.</td>
</tr>
<tr>
<td>vlan-dst-ip</td>
<td>Specifies load distribution based on the VLAN ID and destination IP address.</td>
</tr>
</tbody>
</table>
Specifies load distribution based on the VLAN ID, destination IP address, and TCP/UDP port number.

**vlan-dst-mixed-ip-port**

Specifies load distribution based on the VLAN ID, source and destination IP address.

**vlan-src-dst-ip**

Specifies load distribution based on the VLAN ID, source and destination IP address, and TCP/UDP port number.

**vlan-src-dst-mixed-ip-port**

Specifies load distribution based on the VLAN ID, source IP address.

**vlan-src-ip**

Specifies load distribution based on the VLAN ID, source IP address, and TCP/UDP port number.

**vlan-src-mixed-ip-port**

**Command Default**

The default for Cisco Catalyst 9500 Series Switches is **src-mac**

The default for Cisco Catalyst 9500 High Performance Series Switches is **src-dst-mixed-ip-port**

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can verify your setting by entering either the **show running-config** command in privileged EXEC mode or the **show etherchannel load-balance** command in privileged EXEC mode.

**Note**


**Examples**

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

Device> enable
Device# configure terminal
Device(config)# port-channel load-balance dst-mac
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show etherchannel load-balance</code></td>
<td>Displays information about EtherChannel load balancing.</td>
</tr>
<tr>
<td><code>show running-config</code></td>
<td>Displays the running configuration.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dst-ip</td>
<td>(Optional) Specifies load distribution based on the destination host IP address.</td>
</tr>
<tr>
<td>dst-mac</td>
<td>(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.</td>
</tr>
<tr>
<td>dst-port</td>
<td>(Optional) Specifies load distribution based on the destination TCP/UDP (Layer 4) port number for both IPv4 and IPv6.</td>
</tr>
<tr>
<td>ipv6-label</td>
<td>(Optional) Specifies load distribution based on the source MAC address and IPv6 flow label.</td>
</tr>
<tr>
<td>l3-proto</td>
<td>(Optional) Specifies load distribution based on the source MAC address and Layer 3 protocols.</td>
</tr>
<tr>
<td>src-ip</td>
<td>(Optional) Specifies load distribution based on the source host IP address.</td>
</tr>
<tr>
<td>src-mac</td>
<td>(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.</td>
</tr>
<tr>
<td>src-port</td>
<td>(Optional) Specifies load distribution based on the TCP/UDP (Layer 4) port number.</td>
</tr>
</tbody>
</table>

### Command Default

The default is **src-mac**.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You can verify your setting by entering either the **show running-config** command in privileged EXEC mode or the **show etherchannel load-balance** command in privileged EXEC mode.

### Examples

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

```
Device> enable
Device# configure terminal
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.

```plaintext
port-channel min-links min_links_number
no port-channel min-links
```

**Syntax Description**

| min_links_number | The minimum number of active LACP ports in the port channel. The range is 2 to 8. The default is 1. |

**Command Modes**

- Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` command in privileged EXEC mode 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:

```plaintext
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# port-channel min-links 3
```
**ptp priority1 value**

To specify the priority 1 value to use when advertising a PTP clock, use the `ptp priority1 value` command in global configuration mode.

```
ptp priority1 value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>value</th>
<th>Specifies the priority 1 number to use for this clock.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The range is 0 to 255. The default value is 128.</td>
</tr>
</tbody>
</table>

**Note**

If the value of priority1 is configured to 255, the clock cannot become as Grandmaster.

**Command Default**

Default is 128.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to specify the priority1 value:

```
Device> enable
Device# configure terminal
Device(config)# ptp priority1 120
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptp priority2 value</td>
<td>Specifies the priority 2 number to use for this clock.</td>
</tr>
<tr>
<td>no ptp enable</td>
<td>Disables PTP on an interface.</td>
</tr>
<tr>
<td>ptp profile dot1as</td>
<td>Enables Generalized Precision Time Protocol (gPTP) globally.</td>
</tr>
</tbody>
</table>
To specify the priority 2 number to use when advertising a PTP clock, use the `ptp priority2 value` command in global configuration mode.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Specifies the priority 2 number to use for this clock. The range is 0 to 255. The default value is 128.</td>
</tr>
</tbody>
</table>

### Command Default

Default is 128.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Example

This example shows how to specify the priority2 value:

```
Device> enable
Device# configure terminal
Device(config)# ptp priority 2 120
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ptp priority1 value</code></td>
<td>Specifies the priority 1 number to use for this clock.</td>
</tr>
<tr>
<td><code>no ptp enable</code></td>
<td>Disables PTP on an interface.</td>
</tr>
<tr>
<td><code>ptp profile dot1as</code></td>
<td>Enables Generalized Precision Time Protocol (gPTP) globally.</td>
</tr>
</tbody>
</table>
ptp profile dot1as

To enable Generalized Precision Time Protocol (gPTP) globally, use the `ptp profile dot1as` command in global configuration mode. To disable gPTP, use the `no` form of the command.

```
ptp profile dot1as
no ptp profile dot1as
```

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable gPTP:

```
Device> enable
Device# configure terminal
Device(config)# ptp profile dot1as
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ptp priority1 value</td>
<td>Specifies the priority 1 number to use for this clock.</td>
</tr>
<tr>
<td>ptp priority1 value</td>
<td>Specifies the priority 2 number to use for this clock.</td>
</tr>
<tr>
<td>no ptp enable</td>
<td>Disables PTP on an interface.</td>
</tr>
</tbody>
</table>
mvrp vlan creation

To enable dynamic VLAN creation on a device using Multiple VLAN Registration Protocol (MVRP), use the `mvrp vlan creation` command in global configuration mode. To disable dynamic VLAN creation for MVRP, use the `no` form of this command.

```
mvrp vlan creation
no mvrp vlan creation
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

MVRP is disabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

MVRP dynamic VLAN creation can be used only if Virtual Trunking Protocol (VTP) is in transparent mode.

### Examples

The following example shows a command sequence enabling MVRP dynamic VLAN creation. Notice that the device recognizes that the VTP mode is incorrect and rejects the request for dynamic VLAN creation. Once the VTP mode is changed, MVRP dynamic VLAN creation is allowed.

```
Device(config)# mvrp vlan creation
%Command Rejected: VTP is in non-transparent (server) mode.
Device(config)# vtp mode transparent
Setting device to VTP TRANSPARENT mode.
Device(config)# mvrp vlan creation
%VLAN now may be dynamically created via MVRP/
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mvrp global</td>
<td>Enables MVRP globally on a device.</td>
</tr>
<tr>
<td>vtp mode</td>
<td>Sets the mode for VTP mode on the device.</td>
</tr>
</tbody>
</table>
**mvrp registration**

To set the registrars in a Multiple Registration Protocol (MRP) Attribute Declaration (MAD) instance associated with an interface, use the `mvrp registration` command in global configuration mode. To disable the registrars, use the `no` form of this command.

```plaintext
mvrp registration {normal | fixed | forbidden}
no mvrp registration
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td>Registrar responds normally to incoming Multiple VLAN Registration Protocol (MVRP) messages. Normal is the default state.</td>
</tr>
<tr>
<td>fixed</td>
<td>Registrar ignores all incoming MVRP messages and remains in the IN state.</td>
</tr>
<tr>
<td>forbidden</td>
<td>Registrar ignores all incoming MVRP messages and remains in the EMPTY (MT) state.</td>
</tr>
</tbody>
</table>

**Command Default**

Registrars are set to the normal state.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `mvrp registration` command is operational only if MVRP is configured on an interface.

The `no mvrp registration` command sets the registrar state to the default (normal).

This command can be used to set the registrar in a MAD instance associated with an interface to one of the three states. This command is effective only if MVRP is operational on the interface.

Given that up to 4094 VLANs can be configured on a trunk port, there may be up to 4094 Advanced Services Module (ASM) and Route Switch Module (RSM) pairs in a MAD instance associated with that interface.

**Examples**

The following example sets a fixed, forbidden, and normal registrar on a MAD instance:

```plaintext
Device(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEEE 802.1q trunk ports only.
Device(config)# interface fastethernet2/1
Device(config-if)# mvrp registration fixed
Device(config-if)# interface fastethernet2/2
Device(config-if)# mvrp registration forbidden
Device(config-if)# interface fastethernet2/3
Device(config-if)# no mvrp registration
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mvrp statistics</td>
<td>Clears MVRP-related statistics recorded on one or all MVRP-enabled ports.</td>
</tr>
<tr>
<td><strong>Command</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>debug mvrp</td>
<td>Displays MVRP debugging information.</td>
</tr>
<tr>
<td>mvrp global</td>
<td>Enables MVRP globally on a device and on a particular interface.</td>
</tr>
<tr>
<td>mvrp mac-learning auto</td>
<td>Enables automatic learning of MAC table entries by MVRP.</td>
</tr>
<tr>
<td>mvrp timer</td>
<td>Sets period timers that are used in MRP on a given interface.</td>
</tr>
<tr>
<td>mvrp vlan create</td>
<td>Enables an MVRP dynamic VLAN.</td>
</tr>
<tr>
<td>show mvrp interface</td>
<td>Displays details of the administrative and operational MVRP states of all or one particular IEEE 802.1Q trunk port in the device.</td>
</tr>
<tr>
<td>show mvrp summary</td>
<td>Displays the MVRP configuration at the device level.</td>
</tr>
</tbody>
</table>
**mvrp timer**

To set period timers that are used in Multiple VLAN Registration Protocol (MVRP) on a given interface, use the `mvrp timer` command in interface configuration mode. To remove the timer value, use the `no` form of this command.

```
mvrp timer {join | leave | leave-all | periodic} [centiseconds]
no mvrp timer
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>join</strong></td>
<td>Specifies the time interval between two transmit opportunities that are applied to the Applicant State Machine (ASMs).</td>
</tr>
<tr>
<td><strong>leave</strong></td>
<td>Specifies the duration time before a registrar is moved to EMPTY (MT) state from leave-all (LV) state.</td>
</tr>
<tr>
<td><strong>leave-all</strong></td>
<td>Specifies the time it takes for a LeaveAll timer to expire.</td>
</tr>
<tr>
<td><strong>periodic</strong></td>
<td>Sets the timer value to periodic, a fixed value of 100 centiseconds.</td>
</tr>
<tr>
<td><strong>centiseconds</strong></td>
<td>Timer value measured in centiseconds.</td>
</tr>
<tr>
<td></td>
<td>• Join timer value range is 20 to 10000000.</td>
</tr>
<tr>
<td></td>
<td>• Leave timer value range is 60 to 10000000.</td>
</tr>
<tr>
<td></td>
<td>• LeaveAll timer value range is 10000 and 10000000.</td>
</tr>
<tr>
<td></td>
<td>• Periodic timer value is fixed at 100 centiseconds.</td>
</tr>
</tbody>
</table>

**Command Default**

Join timer value: 20 centiseconds
Leave timer value: 60 centiseconds
LeaveAll timer value: 10000 centiseconds

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `nomvrptimer` command resets the timer value to the default value.

**Examples**

The following example sets the timer levels on an interface:

```
Device(config)# mvrp global
%MVRP is now globally enabled. MVRP is operational on IEE 802.1q trunk ports.
Device(config)# interface GigabitEthernet 6/1
Device(config-if)# mvrp timer join 30
Device(config-if)# mvrp timer leave 70
Device(config-if)# mvrp timer leaveAll 15000
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear mvrp statistics</td>
<td>Clears MVRP-related statistics recorded on one or all MVRP enabled ports.</td>
</tr>
<tr>
<td>debug mvrp</td>
<td>Displays MVRP debugging information.</td>
</tr>
<tr>
<td>mvrp global</td>
<td>Enables MVRP globally on a device and on a particular interface.</td>
</tr>
<tr>
<td>mvrp mac-learning auto</td>
<td>Enables automatic learning of MAC table entries by MVRP.</td>
</tr>
<tr>
<td>mvrp registration</td>
<td>Sets the registrars in a MAD instance associated with an interface.</td>
</tr>
<tr>
<td>mvrp vlan create</td>
<td>Enables an MVRP dynamic VLAN.</td>
</tr>
<tr>
<td>show mvrp interface</td>
<td>Displays details of the administrative and operational MVRP states of all or</td>
</tr>
<tr>
<td></td>
<td>one particular IEEE 802.1q trunk port in the device.</td>
</tr>
<tr>
<td>show mvrp summary</td>
<td>Displays the MVRP configuration at the device level.</td>
</tr>
</tbody>
</table>
rep admin vlan

To configure a Resilient Ethernet Protocol (REP) administrative VLAN for the 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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-id</td>
<td>48-bit static MAC address.</td>
</tr>
</tbody>
</table>

Command Modes

Global configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The range of the REP administrative VLAN is from 1 to 4094.

There can be only one administrative VLAN on a device and on a segment.

Verify your settings by entering the show interfaces rep detail command in privileged EXEC mode.

Examples

The following example shows how to configure VLAN 100 as the REP administrative VLAN:

Device> enable
Device# configure terminal
Device(config)# rep admin vlan 100

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show interfaces rep detail</td>
<td>Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.</td>
</tr>
</tbody>
</table>
rep block port

To configure Resilient Ethernet Protocol (REP) VLAN load balancing on a REP primary edge port, use the rep block port command in interface configuration mode. To return to the default configuration with VLAN 1 as the administrative VLAN, use the no form of this command.

rep block port {id port-id | neighbor-offset | preferred} vlan {vlan-list | all}
no rep block port {id port-id | neighbor-offset | preferred}

Syntax Description

- **id port-id**: Specifies the VLAN blocking alternate port by entering the unique port ID, which is automatically generated when REP is enabled. The REP port ID is a 16-character hexadecimal value.

- **neighbor-offset**: VLAN blocking alternate port by entering the offset number of a neighbor. The range is from -256 to +256. A value of 0 is invalid.

- **preferred**: Selects the regular segment port previously identified as the preferred alternate port for VLAN load balancing.

- **vlan**: Identifies the VLANs to be blocked.

- **vlan-list**: VLAN ID or range of VLAN IDs to be displayed. Enter a VLAN ID from 1 to 4094, or a range or sequence of VLANs (such as 1-3, 22, and 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 the 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

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

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.

Note

- 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 the 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.

### Examples

The following example shows how to configure REP VLAN load balancing:

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep block port id 0009001818D68700 vlan 1-100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show interfaces rep detail</code></td>
<td>Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.</td>
</tr>
</tbody>
</table>
rep lsl-age-timer

To configure the Resilient Ethernet Protocol (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**

<table>
<thead>
<tr>
<th><code>milliseconds</code></th>
<th>REP LSL age-out timer value, in milliseconds (ms). The range is from 120 to 10000 in multiples of 40.</th>
</tr>
</thead>
</table>

**Command Default**

The default LSL age-out timer value is 5 ms.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

**Examples**

The following example shows how to configure a REP LSL age-out timer value:

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge primary
Device(config-if)# rep lsl-age-timer 2000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface interface-type interface-name</td>
<td>Specifies a physical interface or port channel to receive STCNs.</td>
</tr>
<tr>
<td>rep segment</td>
<td>Enables REP on an interface and assigns a segment ID.</td>
</tr>
</tbody>
</table>
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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
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 Resilient Ethernet Protocol (REP) VLAN load balancing is triggered, use the `rep preempt delay` command in interface configuration mode. To remove the configured delay, use the `no` form of this command.

```
rep preempt delay seconds
no rep preempt delay
```

**Syntax Description**

- `seconds` Number of seconds to delay REP preemption. The range is from 15 to 300 seconds. The default is manual preemption without delay.

**Command Default**

REP preemption delay is not set. The default is manual preemption without delay.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter this command on the REP primary edge port.

Enter this command and configure a preempt time delay for VLAN load balancing to be automatically triggered 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 port alerts the alternate port to perform VLAN load balancing (configured by using the `rep block port` command in interface configuration mode) 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` command.

**Examples**

The following example shows how to configure a REP preemption time delay of 100 seconds on the primary edge port:

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep preempt delay 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rep block port</td>
<td>Configures VLAN load balancing.</td>
</tr>
<tr>
<td>show interfaces rep detail</td>
<td>Displays detailed REP configuration and status for all the interfaces or the specified interface, including the administrative VLAN.</td>
</tr>
</tbody>
</table>
rep preempt segment

To manually start Resilient Ethernet Protocol (REP) VLAN load balancing on a segment, use the `rep preempt segment` command in privileged EXEC mode.

```
rep preempt segment segment-id
```

**Syntax Description**

- `segment-id` ID of the REP segment. The range is from 1 to 1024.

**Command Default**

Manual preemption is the default behavior.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter this command on the segment, which has the primary edge port on the device.

Ensure that all the other segment configurations are 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.

Enter the `show rep topology` command in privileged EXEC mode to see which port in the segment is the primary edge port.

If you do not configure VLAN load balancing, entering the `rep preempt segment` `segment-id` command results in the default behavior, that is, the primary edge port blocks all the VLANs.

You can 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.

**Examples**

The following example shows how to manually trigger REP preemption on segment 100:

```
Device> enable
Device# rep preempt segment 100
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>rep block port</code></td>
<td>Configures VLAN load balancing.</td>
</tr>
<tr>
<td><code>rep preempt delay</code></td>
<td>Configures a waiting period after a segment port failure and recovery before REP VLAN load balancing is triggered.</td>
</tr>
<tr>
<td><code>show rep topology</code></td>
<td>Displays REP topology information for a segment or for all the segments.</td>
</tr>
</tbody>
</table>
rep segment

To enable Resilient Ethernet Protocol (REP) on an 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]
```

Command Default
REP is disabled on the interface.

Command Modes
Interface configuration

Command History
```
Release                    Modification
Cisco IOS XE Everest 16.5.1a  This command was introduced.
```

Usage Guidelines
REP ports must be a Layer 2 IEEE 802.1Q port or a 802.1AD port. You must configure two edge ports on each REP segment, a primary edge port and a secondary edge port.

If REP is enabled on two ports on a device, both the ports must be either regular segment ports or edge ports. REP ports follow these rules:

- If only one port on a device is configured in a segment, that port should be an edge port.
- If two ports on a device belong to the same segment, both the ports must be regular segment ports.
- If two ports on a device 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.

Caution
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 that port to be a regular segment port.

### Examples

The following example shows how to enable REP on a regular (nonedge) segment port:

```
Device> enable
Device# configure terminal
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> enable
Device# configure terminal
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> enable
Device# configure terminal
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> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep segment 1 edge no-neighbor primary
```
**rep stcn**

To configure a Resilient Ethernet Protocol (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 task of sending 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 REP 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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can verify your settings by entering the `show interfaces rep detail` command in privileged EXEC mode.

**Examples**

The following example shows how to configure a REP edge port to send STCNs to segments 25 to 50:

```
Device> enable
Device# configure terminal
Device(config)# interface TenGigabitEthernet 4/1
Device(config-if)# rep stcn segment 25-50
```
show avb domain

To display the AVB domain information, use the **show avb domain** command.

**show avb domain**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration mode (#)

**Example:**

The following is sample output from the **show avb domain** command:

```
Device# show avb domain

AVB Class-A
Priority Code Point : 3
VLAN : 2
Core ports : 1
Boundary ports : 67

AVB Class-B
Priority Code Point : 2
VLAN : 2
Core ports : 1
Boundary ports : 67

+-------------------------------+-------------------+------------------------+-------------------+------------------------+---+-------------------+------------------------+
<table>
<thead>
<tr>
<th>Interface</th>
<th>State</th>
<th>Delay</th>
<th>PCP</th>
<th>VID</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/1</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/2</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/3</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/4</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/5</td>
<td>up</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Port is not asCapable</td>
</tr>
<tr>
<td>Te1/0/6</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/7</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/8</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/9</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/10</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/11</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/12</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/13</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/14</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/15</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/16</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/17</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/18</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/19</td>
<td>up</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Port is not asCapable</td>
</tr>
<tr>
<td>Te1/0/20</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/21</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/22</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/23</td>
<td>up</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Port is not asCapable</td>
</tr>
<tr>
<td>Te1/0/24</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/25</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/26</td>
<td>down</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Oper state not up</td>
</tr>
</tbody>
</table>
```

---

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Oper state</th>
<th>Additional info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Te1/0/27</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/28</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/29</td>
<td>up</td>
<td>N/A</td>
<td>Port is not asCapable</td>
</tr>
<tr>
<td>Te1/0/30</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/31</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/32</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/33</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/34</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/35</td>
<td>up</td>
<td>N/A</td>
<td>Port is not asCapable</td>
</tr>
<tr>
<td>Te1/0/36</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/37</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/38</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/39</td>
<td>up</td>
<td>507ns</td>
<td></td>
</tr>
<tr>
<td>Class- A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Class- B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Core 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Te1/0/40</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/41</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/42</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/43</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/44</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/45</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/46</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/47</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/0/48</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/1</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/2</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/3</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/4</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/5</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/6</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/7</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/8</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/9</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/10</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/11</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/12</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/13</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/14</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/15</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Te1/1/16</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Fo1/1/1</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Fo1/1/2</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Fo1/1/3</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
<tr>
<td>Fo1/1/4</td>
<td>down</td>
<td>N/A</td>
<td>Oper state not up</td>
</tr>
</tbody>
</table>

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show avb streams

To display the AVB stream information, use the `show avb streams` command.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration mode (#)

**Example:**

The following is sample output from the `show avb streams` command:

```
Device# show avb streams

Stream ID: 0011.0100.0001:1  Incoming Interface: Te1/1/1
  Destination : 91E0.F000.FE00
  Class        : A
  Rank         : 1
  Bandwidth    : 6400 Kbit/s

  Outgoing Interfaces:
  Interface  State   Time of Last Update Information
  -------  --------  ----------------------  ----------------------
  Te1/1/1    Ready    Tue Apr 26 01:25:40.634

Stream ID: 0011.0100.0002:2  Incoming Interface: Te1/1/1
  Destination : 91E0.F000.FE01
  Class        : A
  Rank         : 1
  Bandwidth    : 6400 Kbit/s

  Outgoing Interfaces:
  Interface  State   Time of Last Update Information
  -------  --------  ----------------------  ----------------------
  Te1/1/1    Ready    Tue Apr 26 01:25:40.634
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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}}]

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>channel-group-number</code></td>
<td>(Optional) Channel group number. The range is 1 to 128.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed EtherChannel information.</td>
</tr>
<tr>
<td><code>load-balance</code></td>
<td>(Optional) Displays the load-balance or frame-distribution scheme among ports in the port channel.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>(Optional) Displays EtherChannel port information.</td>
</tr>
<tr>
<td><code>port-channel</code></td>
<td>(Optional) Displays port-channel information.</td>
</tr>
<tr>
<td><code>protocol</code></td>
<td>(Optional) Displays the protocol that is being used in the channel.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>(Optional) Displays a one-line summary per channel group.</td>
</tr>
</tbody>
</table>

Command Modes

User EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not specify a channel group number, all channel groups are displayed.

In the output, the passive port list field is displayed only for Layer 3 port channels. This field means that the physical port, which is still not up, is configured to be in the channel group (and indirectly is in the only port channel in the channel group).

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
                   Port-channel = 1 Mode = Active Gcchange = -
                   Port index = 0 Load = 0x00 Protocol = LACP
                   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.
```
Local information:

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Priority</th>
<th>Key</th>
<th>Key</th>
<th>Number</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x1</td>
<td>0x1</td>
<td>0x101</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>A</td>
<td>bndl</td>
<td>32768</td>
<td>0x0</td>
<td>0x1</td>
<td>0x0</td>
<td>0x3D</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Gi1/0/1</td>
<td>Active</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Gi1/0/2</td>
<td>Active</td>
<td>0</td>
</tr>
</tbody>
</table>

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:
```
<table>
<thead>
<tr>
<th>Index</th>
<th>Load</th>
<th>Port</th>
<th>EC state</th>
<th>No of bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00</td>
<td>Gi1/0/1</td>
<td>Active</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>00</td>
<td>Gi1/0/2</td>
<td>Active</td>
<td>0</td>
</tr>
</tbody>
</table>

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 Resilient Ethernet Protocol (REP) configuration and status for all interfaces or a specified interface, including the administrative VLAN, use the **show interfaces rep detail** command in privileged EXEC mode.

```plaintext
show interfaces [interface-id] rep detail
```

**Syntax Description**

- **interface-id** (Optional) Physical interface used to display the port ID.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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** command in privileged EXEC mode.

**Examples**

The following example shows how to display the REP configuration and status for a specified interface:

```
Device> enable
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
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rep admin vlan</td>
<td>Configures a REP administrative VLAN for the REP to transmit HFL messages.</td>
</tr>
</tbody>
</table>
show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the `show lacp` command in user EXEC mode.

```
show lacp [channel-group-number] {counters | internal | neighbor | sys-id}
```

**Syntax Description**

- **channel-group-number** (Optional) Channel group number. The range is 1 to 128.
- **counters** Displays traffic information.
- **internal** Displays internal information.
- **neighbor** Displays neighbor information.
- **sys-id** Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.

**Command Modes**

User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Port</th>
<th>LACPDUs Sent</th>
<th>Marker Sent</th>
<th>LACPDUs Recv</th>
<th>Marker Recv</th>
<th>LACPDUs Pkts</th>
<th>LACPDUs Err</th>
</tr>
</thead>
<tbody>
<tr>
<td>G12/0/1</td>
<td>19</td>
<td>0</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>G12/0/2</td>
<td>14</td>
<td>0</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Table 94: show lacp counters Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LACPDUs Sent and Recv</td>
<td>The number of LACP packets sent and received by a port.</td>
</tr>
<tr>
<td>Marker Sent and Recv</td>
<td>The number of LACP marker packets sent and received by a port.</td>
</tr>
</tbody>
</table>
The number of LACP marker response packets sent and received by a port.

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 LACPDU
        F - Device is requesting Fast LACPDU
        A - Device is in Active mode
        P - Device is in Passive mode

Channel group 1

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>LACP port</th>
<th>Admin</th>
<th>Oper</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/1</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x3</td>
<td>0x3</td>
<td>0x4</td>
<td>0x3D</td>
</tr>
<tr>
<td>Gi2/0/2</td>
<td>SA</td>
<td>bndl</td>
<td>32768</td>
<td>0x3</td>
<td>0x3</td>
<td>0x5</td>
<td>0x3D</td>
</tr>
</tbody>
</table>
```

The following table describes the fields in the display:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>State of the specific port. These are the allowed values:</td>
</tr>
<tr>
<td></td>
<td>• — — Port is in an unknown state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>bndl</strong> — Port is attached to an aggregator and bundled with other ports.</td>
</tr>
<tr>
<td></td>
<td>• <strong>susp</strong> — Port is in a suspended state; it is not attached to any aggregator.</td>
</tr>
<tr>
<td></td>
<td>• <strong>hot-sby</strong> — Port is in a hot-standby state.</td>
</tr>
<tr>
<td></td>
<td>• <strong>indiv</strong> — Port is incapable of bundling with any other port.</td>
</tr>
<tr>
<td></td>
<td>• <strong>indep</strong> — 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).</td>
</tr>
<tr>
<td></td>
<td>• <strong>down</strong> — Port is down.</td>
</tr>
</tbody>
</table>

| 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 | State variables for the port, encoded as individual bits within a single octet with these meanings:
- bit0: LACP_Activity
- bit1: LACP_Timeout
- bit2: Aggregation
- bit3: Synchronization
- bit4: Collecting
- bit5: Distributing
- bit6: Defaulted
- bit7: Expired

Note: In the list above, bit7 is the MSB and bit0 is the LSB.

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

```
Device> show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs  F - Device is sending Fast LACPDUs
         A - Device is in Active mode         P - Device is in Passive mode

Channel group 3 neighbors

Partner’s information:

<table>
<thead>
<tr>
<th>Port</th>
<th>System ID</th>
<th>Port Number</th>
<th>Age</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/1</td>
<td>32768,0007.eb49.5e80</td>
<td>0xC</td>
<td>19s</td>
<td>SP</td>
</tr>
<tr>
<td></td>
<td>LACP Partner</td>
<td>Partner</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Priority</td>
<td>Oper Key</td>
<td>Port State</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32768</td>
<td>0x3</td>
<td>0x3c</td>
<td></td>
</tr>
</tbody>
</table>

Partner’s information:
```
<table>
<thead>
<tr>
<th>Partner</th>
<th>System ID</th>
<th>Partner</th>
<th>Port Number</th>
<th>Age</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>System ID</td>
<td>Partner</td>
<td>Port Number</td>
<td>Age</td>
<td>Flags</td>
</tr>
<tr>
<td>Gi2/0/2</td>
<td>32768,0007.eb49.5e80</td>
<td>0xD</td>
<td>15s</td>
<td>SP</td>
<td></td>
</tr>
</tbody>
</table>

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 msrp port bandwidth

To display Multiple Stream Reservation Protocol (MSRP) port bandwidth information, use the `show msrp port bandwidth` command.

**show msrp port bandwidth**

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Command Modes

Global configuration mode (#)

### Example:

The following is sample output from the `show msrp port bandwidth` command:

```
Device# show msrp port bandwidth

Ethernet Capacity Assigned Available Reserved
Interface (Kbit/s) A | B A | B A | B A | B
------------------------------------------------------------------
Te1/0/1 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/2 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/3 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/4 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/5 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/6 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/8 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/9 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/10 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/11 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/12 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/13 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/14 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/15 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/16 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/17 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/18 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/19 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/20 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/21 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/22 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/23 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/0/24 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Gi1/1/1 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Gi1/1/2 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Gi1/1/3 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Gi1/1/4 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/1 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/2 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/3 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/4 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/5 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/6 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/7 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Te1/1/8 10000000 | 75 | 0 75 | 75 | 75 | 0 | 0
Fo1/1/1 40000000 | 75 | 0 75 | 75 | 75 | 0 | 0
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
<table>
<thead>
<tr>
<th>Port</th>
<th>Bandwidth</th>
<th>Used</th>
<th>Port</th>
<th>Free</th>
<th>Used</th>
<th>Free</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fo1/1/2</td>
<td>40000000</td>
<td>75</td>
<td>0</td>
<td>75</td>
<td>75</td>
<td>0</td>
</tr>
</tbody>
</table>
**show msrp streams**

To display information about the Multiple Stream Reservation Protocol (MSRP) streams, use the `show msrp streams` command.

```
show msrp streams [ detailed | brief ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detailed</td>
<td>Displays detailed MSRP stream information.</td>
</tr>
<tr>
<td>brief</td>
<td>Displays MSRP stream information in brief.</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration mode (#)

**Example:**

The following is sample output from the `show msrp streams` command:

```
Device# show msrp streams

Stream ID Talker Listener
Advertise Fail Ready ReadyFail AskFail
R | D R | D R | D R | D

yy:yy:yy:yy:yy:yy:0001 1 | 2 0 | 0 1 | 0 0 | 1 1 | 0
zz:zz:zz:zz:zz:zz:0002 1 | 0 0 | 1 1 | 0 0 | 0 0 | 1
```

The following is sample output from the `show msrp streams detailed` command:

```
Device# show msrp streams detailed

Stream ID: 0011.0100.0001:1
Stream Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
Create Time: Mon Apr 25 23:41:11.413
Destination Address: 91E0.F000.FE00
VLAN Identifier: 1
Data Frame Priority: 3 (Class A)
MaxFrameSize: 100
MaxIntervalFrames: 1 frames/125us
Stream Bandwidth: 6400 Kbit/s
Rank: 1
Received Accumulated Latency: 20
Stream Attributes Table:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Attr</th>
<th>State</th>
<th>Direction</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Register</td>
<td>Talker</td>
<td>Advertise</td>
<td></td>
</tr>
</tbody>
</table>

Attribute Age: 01:57:46 (since Mon Apr 25 23:41:11.413)
MRP Applicant: Very Anxious Observer, send None
MRP Registrar: In
Accumulated Latency: 20
```
The following is sample output from the `show msrp streams brief` command:

Device# show msrp streams brief

Legend: R = Registered, D = Declared.

<table>
<thead>
<tr>
<th>Stream ID</th>
<th>Destination Address</th>
<th>Bandwidth (Kbit/s)</th>
<th>Talkers R</th>
<th>D</th>
<th>Listeners R</th>
<th>D</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>0011.0100.0001:1</td>
<td>91E0.F000.FE00</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0002:2</td>
<td>91E0.F000.FE01</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0003:3</td>
<td>91E0.F000.FE02</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0004:4</td>
<td>91E0.F000.FE03</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0005:5</td>
<td>91E0.F000.FE04</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0006:6</td>
<td>91E0.F000.FE05</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0007:7</td>
<td>91E0.F000.FE06</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0008:8</td>
<td>91E0.F000.FE07</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.0009:9</td>
<td>91E0.F000.FE08</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
<tr>
<td>0011.0100.000A:10</td>
<td>91E0.F000.FE09</td>
<td>6400</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>No</td>
</tr>
</tbody>
</table>
**show pagp**

To display Port Aggregation Protocol (PAgP) channel-group information, use the `show pagp` command in EXEC mode.

```
show pagp [channel-group-number] {counters | dual-active | internal | neighbor}
```

**Syntax Description**

- **channel-group-number** *(Optional)* Channel group number. The range is 1 to 128.
- **counters** Displays traffic information.
- **dual-active** Displays the dual-active status.
- **internal** Displays internal information.
- **neighbor** Displays neighbor information.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 SentRecv SentRecv
----------------------------------------
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

<table>
<thead>
<tr>
<th>Port</th>
<th>Detect Capable</th>
<th>Name</th>
<th>Partner</th>
<th>Port</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>No</td>
<td>-p2</td>
<td>Gi3/0/3</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>No</td>
<td>-p2</td>
<td>Gi3/0/4</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Flags</th>
<th>State</th>
<th>Timers</th>
<th>Interval</th>
<th>Partner PAgP Learning Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1 128 Any 16</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>SC</td>
<td>U6/S7</td>
<td>H</td>
<td>30s</td>
<td>1 128 Any 16</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Partner</th>
<th>Device ID</th>
<th>Partner</th>
<th>Port</th>
<th>Age</th>
<th>Flags</th>
<th>Cap.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>-p2</td>
<td>0002.4b29.4600</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>-p2</td>
<td>0002.4b29.4600</td>
<td>Gi1/0/2</td>
<td>24s</td>
<td>SC</td>
<td>10001</td>
<td></td>
</tr>
</tbody>
</table>
show platform etherchannel

To display platform-dependent EtherChannel information, use the `show platform etherchannel` command in privileged EXEC mode.

```
show platform etherchannel channel-group-number {group-mask | load-balance mac src-mac dst-mac [ip src-ip dst-ip [port src-port dst-port]]} [switch switch-number]
```

**Syntax Description**

- `channel-group-number`: Channel group number. The range is 1 to 128.
- `group-mask`: Displays EtherChannel group mask.
- `mac src-mac dst-mac`: Specifies the source and destination MAC addresses.
- `ip src-ip dst-ip`: (Optional) Specifies the source and destination IP addresses.
- `port src-port dst-port`: (Optional) Specifies the source and destination layer port numbers.
- `switch switch-number`: (Optional) Specifies the stack member.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 hardware fed active vlan ingress

To display if native vlan tagging is enabled or disabled for a particular vlan, use the **show platform hardware fed active vlan ingress**

**show platform hardware fed active vlan vlan ID ingress**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan vlan ID</code></td>
<td>Specifies the VLAN ID.</td>
</tr>
<tr>
<td><code>ingress</code></td>
<td>Specifies Spanning Tree Protocol (STP) state information in ingress direction.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC mode (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

The following is sample output from the **show platform hardware fed active vlan ingress** command:

```
Device# show platform hardware fed active vlan 1 ingress
VLAN STP State in hardware
vlan id is: 1
Interfaces in forwarding state: Hu1/0/45(Tagged)
flood list: Hu1/0/45
```
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}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>etherchannel channel-group-number group-mask</td>
<td>Displays the EtherChannel group-mask table for the specified channel group. The range is 1 to 128.</td>
</tr>
<tr>
<td>interface-numbers</td>
<td>Displays interface numbers information.</td>
</tr>
<tr>
<td>port-data interface-id</td>
<td>Displays port data information for the specified interface.</td>
</tr>
<tr>
<td>port-state</td>
<td>Displays port state information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 platform software fed switch ptp**

To display information about ptp status on the port, use the `show platform software fed switch ptp` command.

```
show platform software fed switch { switch-number | active | standby } ptp { domain domain-value | if-id value | test }
```

### Syntax Description

- **switch switch-number**
  - Displays information about the switch. Valid values for `switch-number` argument are from 0 to 9.
- **active**
  - Displays information about the active instance of the switch.
- **standby**
  - Displays information about the standby instance of the switch.
- **domain domain-value**
  - Displays information about the specified domain.
- **if-id value**
  - Displays information about the specified interface.
- **test**
  - Executes ptp test

### Command History

**Release**

- Cisco IOS XE Fuji 16.8.1a

**Modification**

- This command was introduced.

### Command Modes

Global configuration mode (#)

### Example:

The following is sample output from the `show platform software fed switch active ptp if-id 0x20` command:

```
Device# show platform software fed switch active ptp if-id 0x20

Displaying port data for if_id 20
----------------------------------------------------------
Port Mac Address 04:6C:9D:4E:3A:9A
Port Clock Identity 04:6C:9D:FF:FE:4E:3A:80
Port number 28
PTP Version 2
domain_value 0
dot1as_capable: FALSE
sync_recpt_timeout_time_interval 375000000 nanoseconds
sync_interval 125000000 nanoseconds
neighbor_rate_ratio 0.000000
neighbor_prop_delay 0 nanoseconds
compute_neighbor_rate_ratio: TRUE
compute_neighbor_prop_delay: TRUE
port_enabled: TRUE
ptt_port_enabled: TRUE
current_log_pdelay_req_interval 0
pdelay_req_interval 0 nanoseconds
allowed_lost_responses 3
neighbor_prop_delay_threshold 2000 nanoseconds
```

is_measuring_delay : FALSE
Port state: MASTER
sync_seq_num 22023
delay_req_seq_num 23857
num sync messages transmitted  0
num sync messages received  0
num followup messages transmitted  0
num followup messages received  0
num pdelay requests transmitted 285695
num pdelay requests received  0
num pdelay responses transmitted  0
num pdelay responses received  0
num pdelay followup responses transmitted  0
num pdelay followup responses received  0
show ptp brief

To display a brief status of ptp on the interfaces, use the `show ptp brief` command in global configuration mode.

**show ptp brief**

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Command Modes**

Global configuration mode (#)

---

**Example:**

The following is sample output from the `show ptp brief` command:

```
Device# show ptp brief

Interface   Domain  PTP State
FortyGigabitEthernet1/1/1    0       FAULTY
FortyGigabitEthernet1/1/2    0       SLAVE
GigabitEthernet1/1/1         0       FAULTY
GigabitEthernet1/1/2         0       FAULTY
GigabitEthernet1/1/3         0       FAULTY
GigabitEthernet1/1/4         0       FAULTY
TenGigabitEthernet1/0/1      0       FAULTY
TenGigabitEthernet1/0/2      0       FAULTY
TenGigabitEthernet1/0/3      0       MASTER
TenGigabitEthernet1/0/4      0       FAULTY
TenGigabitEthernet1/0/5      0       FAULTY
TenGigabitEthernet1/0/6      0       FAULTY
TenGigabitEthernet1/0/7      0       MASTER
TenGigabitEthernet1/0/8      0       FAULTY
TenGigabitEthernet1/0/9      0       FAULTY
TenGigabitEthernet1/0/10     0       FAULTY
TenGigabitEthernet1/0/11     0       MASTER
TenGigabitEthernet1/0/12     0       FAULTY
TenGigabitEthernet1/0/13     0       FAULTY
TenGigabitEthernet1/0/14     0       FAULTY
TenGigabitEthernet1/0/15     0       FAULTY
TenGigabitEthernet1/0/16     0       FAULTY
```

---

Layer 2/3
show ptp clock

To display ptp clock information, use the **show ptp clock** command in global configuration mode.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Command Modes

Global configuration mode (#)

### Example:

The following is sample output from the **show ptp clock** command:

```
Device# show ptp clock

PTP CLOCK INFO
  PTP Device Type: Boundary clock
  PTP Device Profile: IEEE 802/1AS Profile
  Clock Identity: 0x4:6C:9D:FF:FE:4F:95:0
  Clock Domain: 0
  Number of PTP ports: 38
  PTP Packet priority: 4
  Priority1: 128
  Priority2: 128
  Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): 16640
  Offset From Master(ns): 0
  Mean Path Delay(ns): 0
  Steps Removed: 3
  Local clock time: 00:12:13 UTC Jan 1 1970
```
show ptp parent

To display the parent clock information, use the `show ptp parent` command in global configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration mode (#)

**Example:**

The following is sample output from the `show ptp parent` command:

```
Device# show ptp parent
Steps Removed: 3
Local clock time: 00:12:13 UTC Jan 1 1970

This command can be used to view the parent clock information.

Device#show ptp parent

PTP PARENT PROPERTIES
Parent Clock:
  Parent Clock Identity: 0xB0:7D:47:FF:FE:9E:B6:80
  Parent Port Number: 3
  Observed Parent Offset (log variance): 16640
  Observed Parent Clock Phase Change Rate: N/A

Grandmaster Clock:
  Grandmaster Clock Identity: 0x4:6C:9D:FF:FE:67:3A:80
  Grandmaster Clock Quality:
    Class: 248
    Accuracy: Unknown
    Offset (log variance): 16640
    Priority1: 0
    Priority2: 128
```
show ptp port

To display the ptp port information, use the **show ptp port** command in global configuration mode.

**Example:**

The following is sample output from the **show ptp port** command:

```
Device# show ptp port

PTP PORT DATASET: FortyGigabitEthernet1/1/1
  Port identity: port number: 1
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt timeout: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  Sync interval(log mean): 0
  Delay Mechanism: End to End
  Peer delay request interval(log mean): 0
  Sync fault limit: 50000000

PTP PORT DATASET: FortyGigabitEthernet1/1/2
  Port identity: port number: 2
  PTP version: 2
  Port state: FAULTY
  Delay request interval(log mean): 5
  Announce receipt timeout: 3
  Peer mean path delay(ns): 0
  Announce interval(log mean): 1
  --More--
```

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Command Modes**

Global configuration mode (#)
show rep topology

To display Resilient Ethernet Protocol (REP) topology information for a segment or for all the 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>segment</code></td>
<td>(Optional) Specifies the segment for which to display the REP topology information. The <code>segment-id</code> range is from 1 to 1024.</td>
</tr>
<tr>
<td><code>archive</code></td>
<td>(Optional) Displays the previous topology of the segment. This keyword is useful for troubleshooting a link failure.</td>
</tr>
<tr>
<td><code>detail</code></td>
<td>(Optional) Displays detailed REP topology information.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a 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 a 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
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Port Priority: 000
Neighbor Number: 1 / [-6]
10.64.106.228, Te3/4 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 010
  Port Priority: 000
Neighbor Number: 2 / [-5]
10.64.106.228, Te3/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b1b.1f20
  Port Number: 00E
  Port Priority: 000
Neighbor Number: 3 / [-4]
10.64.106.67, Te4/3 (Intermediate)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1800
  Port Number: 008
  Port Priority: 000
Neighbor Number: 4 / [-3]
10.64.106.67, Te4/4 (Intermediate)
  Alternate Port, some vlans blocked
  Bridge MAC: 0005.9b2e.1800
  Port Number: 00A
  Port Priority: 000
Neighbor Number: 5 / [-2]
10.64.106.63, Te4/4 (Secondary Edge)
  Open Port, all vlans forwarding
  Bridge MAC: 0005.9b2e.1700
  Port Number: 00A
  Port Priority: 000
Neighbor Number: 6 / [-1]
show udld

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

```
show udld [ANI | AccessTunnel | Auto-Template | BDI | CEM-PG | GMPLS | GigabitEthernet | HundredGigE | InternalInterface | LISP | Loopback | Null | PROTECTION_GROUP | Port-channel | SDH_ACR | SERIAL-ACR | Serial-PG | TLS-VIF | Tunnel | Tunnel-tp | TwentyFiveGigE | VirtualPortGroup | Vlan | nve] interface_number
```

**show udld neighbors**

**show udld fast-hello** `interface_number`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANI</td>
<td>(Optional) Displays UDLD operational status of the Autonomic-Networking virtual interface.</td>
</tr>
<tr>
<td>Auto-Template</td>
<td>(Optional) Displays UDLD operational status of the auto-template interface. The range is from 1 to 999.</td>
</tr>
<tr>
<td>BDI</td>
<td>(Optional) Displays UDLD operational status of the Bridge-Domain interface.</td>
</tr>
<tr>
<td>CEM-PG</td>
<td>(Optional) Displays UDLD operational status of the Circuit Emulation interface with Protection group.</td>
</tr>
<tr>
<td>GMPLS</td>
<td>(Optional) Displays UDLD operational status of the MPLS interface.</td>
</tr>
<tr>
<td>GigabitEthernet</td>
<td>(Optional) Displays UDLD operational status of the GigabitEthernet interface.</td>
</tr>
<tr>
<td>HundredGigE</td>
<td>(Optional) Displays UDLD operational status of the Hundred Gigabit Ethernet.</td>
</tr>
<tr>
<td>InternalInterface</td>
<td>(Optional) Displays UDLD operational status of the internal interface. The range is from 0 to 9.</td>
</tr>
<tr>
<td>Loopback</td>
<td>(Optional) Displays UDLD operational status of the loopback interface. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td>Null</td>
<td>(Optional) Displays UDLD operational status of the null interface.</td>
</tr>
<tr>
<td>PROTECTION_GROUP</td>
<td>(Optional) Displays UDLD operational status of the Protection-group controller.</td>
</tr>
<tr>
<td>Port-channel</td>
<td>(Optional) Displays UDLD operational status of the Ethernet channel interfaces. The range is from 1 to 128.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SDH_ACR</td>
<td>(Optional) Displays UDLD operational status of the Virtual SDH-ACR controller.</td>
</tr>
<tr>
<td>SERIAL-ACR</td>
<td>(Optional) Displays UDLD operational status of the Serial interface with ACR.</td>
</tr>
<tr>
<td>TLS-VIF</td>
<td>(Optional) Displays UDLD operational status of the TLS Virtual Interface.</td>
</tr>
<tr>
<td>Tunnel</td>
<td>(Optional) Displays UDLD operational status of the tunnel interface. The range is from 0 to 2147483647.</td>
</tr>
<tr>
<td>Tunnel-tp</td>
<td>(Optional) Displays UDLD operational status of the MPLS Transport Profile interface.</td>
</tr>
<tr>
<td>TwentyFiveGigE</td>
<td>(Optional) Displays UDLD operational status of the Twenty Five Gigabit Ethernet.</td>
</tr>
<tr>
<td>VirtualPortGroup</td>
<td>(Optional) Displays UDLD operational status of the Virtual Port Group.</td>
</tr>
<tr>
<td>Vlan</td>
<td>(Optional) Displays UDLD operational status of the VLAN interface. The range is from 1 to 4095.</td>
</tr>
<tr>
<td>interface_number</td>
<td>(Optional) ID of the interface and port number. Valid interfaces include physical ports, VLANs, and port channels.</td>
</tr>
<tr>
<td>nve</td>
<td>(Optional) Displays UDLD operational status of Network virtualization endpoint interface</td>
</tr>
<tr>
<td>neighbors</td>
<td>(Optional) Displays neighbor information only.</td>
</tr>
<tr>
<td>fast-hello</td>
<td>(Optional) Displays ports that have fast-hello configured and their fast-hello operational status.</td>
</tr>
<tr>
<td>fast-hello interface_number</td>
<td>(Optional) Displays the fast-hello information of a specific interface.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The fast-hello keyword was added to the command.</td>
</tr>
</tbody>
</table>
If you do not enter an interface ID, administrative and operational UDLD status for all interfaces appear.

Examples:

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.

```
Device> show udld TwentyFiveGigE1/0/1
Interface TwentyFiveGigE1/0/1
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 7000 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Enabled
Port fast-hello interval: 200 ms
Port fast-hello operational state: Enabled
Neighbor fast-hello configuration setting: Enabled
Neighbor fast-hello interval: 200 ms

Entry 1
---
Expiration time: 1400 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: 0A74286120
Port ID: Hu1/0/2
Neighbor echo 1 device: 0A74286A80
Neighbor echo 1 port: Hu1/0/10

TLV Message interval: 15
TLV fast-hello interval: 500 ms
TLV Time out interval: 5
TLV CDP Device name: SkyFox-59
```

This is an example of output from the `show udld fast-hello interface-id` command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. The fast-hello information of the port is displayed along with the UDLD operational status.

```
Device> show udld fast-hello hundredGigE 1/0/10
Interface hundredGigE 1/0/10
---
Port enable administrative configuration setting: Enabled
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single neighbor detected
Message interval: 500 ms
Time out interval: 5000 ms

Port fast-hello configuration setting: Enabled
Port fast-hello interval: 500 ms
Port fast-hello operational state: Enabled
Neighbor fast-hello configuration setting: Enabled
Neighbor fast-hello interval: 500 ms

Entry 1
---
Expiration time: 1400 ms
Cache Device index: 1
Current neighbor state: Bidirectional
Device ID: 0A74286120
Port ID: Hu1/0/2
```

Layer 2/3
Neighbor echo 1 device: 0A74286A80
Neighbor echo 1 port: Hu1/0/10

TLV Message interval: 15
TLV fast-hello interval: 500 ms
TLV Time out interval: 5
TLV CDP Device name: SkyFox-59

This is an example of output from the `show udld fast-hello` global command.

Device> show udld fast-hello
Total ports on which fast hello can be configured: 32
Total ports with fast hello configured: 3
Total ports with fast hello operational: 3
Total ports with fast hello non-operational: 0

<table>
<thead>
<tr>
<th>Port-ID</th>
<th>Hello</th>
<th>Neighbor-Hello</th>
<th>Neighbor-Device</th>
<th>Neighbor-Port</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hu1/0/10</td>
<td>500</td>
<td>500</td>
<td>0A74286120</td>
<td>Hu1/0/2</td>
<td>Operational</td>
</tr>
<tr>
<td>Hu1/0/12</td>
<td>500</td>
<td>500</td>
<td>0A74286120</td>
<td>Hu1/0/18</td>
<td>Operational</td>
</tr>
<tr>
<td>Hu1/0/14</td>
<td>500</td>
<td>500</td>
<td>0A74286120</td>
<td>Hu1/0/4</td>
<td>Operational</td>
</tr>
</tbody>
</table>

This is an example of output from the `show udld neighbors` command:

Device> enable
Device# show udld neighbors

<table>
<thead>
<tr>
<th>Port</th>
<th>Device Name</th>
<th>Device ID</th>
<th>Port-ID</th>
<th>OperState</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/1</td>
<td>Switch-A</td>
<td>1</td>
<td>Gi2/0/1</td>
<td>Bidirectional</td>
</tr>
<tr>
<td>Gi3/0/1</td>
<td>Switch-A</td>
<td>2</td>
<td>Gi3/0/1</td>
<td>Bidirectional</td>
</tr>
</tbody>
</table>
show vlan dot1q tag native

To display the status of tagging on the native VLAN use the `show vlan dot1q tag native` command.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC mode (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td></td>
</tr>
</tbody>
</table>

Example

The following is sample output from the `show vlan dot1q tag native` command:

```
Device# show vlan dot1q tag native
*Feb 1 06:47:30.719: %SYS-5-CONFIG_I: Configured from console by console
dot1q native vlan tagging is enabled globally

Per Port Native Vlan Tagging State
---------------------------------------

<table>
<thead>
<tr>
<th>Port</th>
<th>Operational Mode</th>
<th>Native VLAN Tagging State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hu1/0/45</td>
<td>trunk</td>
<td>enabled</td>
</tr>
</tbody>
</table>
```
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**

**Command Default**

By default, all interfaces are in Layer 2 mode.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport
```
**switchport access vlan**

To configure a port as a static-access port, use the `switchport access vlan` command in interface configuration mode. To reset the access mode to the default VLAN mode for the device, use the `no` form of this command.

```
switchport access vlan {vlan-id }
no switchport access vlan
```

**Syntax Description**

- **vlan-id**  
  VLAN ID of the access mode VLAN; the range is 1 to 4094.

**Command Default**

The default access VLAN and trunk interface native VLAN is a default VLAN corresponding to the platform or interface hardware.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport access vlan 2
```
# switchport mode

To configure the VLAN membership mode of a port, use the `switchport mode` command in interface configuration mode. To reset the mode to the appropriate default for the device, use the `no` form of this command.

```
switchport mode {access | dynamic | {auto | desirable} | trunk}
no switchport mode {access | dynamic | {auto | desirable} | trunk}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>access</strong></td>
<td>Sets the port to access mode (either static-access or dynamic-access depending on the setting of the <code>switchport access vlan</code> 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.</td>
</tr>
<tr>
<td><strong>dynamic auto</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>dynamic desirable</strong></td>
<td>Sets the port trunking mode dynamic parameter to desirable to specify that the interface actively attempt to convert the link to a trunk link.</td>
</tr>
<tr>
<td><strong>trunk</strong></td>
<td>Sets the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router.</td>
</tr>
</tbody>
</table>

## Command Default

The default mode is **dynamic auto**.

## Command Modes

Interface configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

A configuration that uses the `access` or `trunk` keywords takes effect only when you configure the port in the appropriate mode by using the `switchport mode` command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change.

When you enter **dynamic auto** mode, the interface converts the link to a trunk link if the neighboring interface is set to **trunk** or **desirable** mode.

When you enter **dynamic desirable** mode, the interface becomes a trunk interface if the neighboring interface is set to **trunk**, **desirable**, or **auto** mode.
To autonegotiate trunking, the interfaces must be in the same VLAN Trunking Protocol (VTP) domain. Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly, which could cause misconfigurations. To avoid this problem, configure interfaces connected to devices that do not support DTP to not forward DTP frames, which turns off DTP.

- If you do not intend to trunk across those links, use the `switchport mode access` command in interface configuration mode to disable trunking.
- To enable trunking to a device that does not support DTP, use the `switchport mode trunk` and `switchport nonegotiate` commands in interface configuration mode 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` command in privileged EXEC mode and examining information in the `Administrative Mode` and `Operational Mode` rows.

**Examples**

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

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport mode access
```

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

```
Device> enable
Device# configure terminal
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> enable
Device# configure terminal
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
```

**Command Default**

The default is to use DTP negotiation to learn the trunking status.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 `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> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/1
Device(config-if)# switchport nonegotiate
```

You can verify your setting by entering the `show interfaces interface-id switchport` command in privileged EXEC mode.
### 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.

#### Note

The keyword `native vlan tag` is supported only on Cisco Catalyst 9500 Series Switches - High Performance.

```plaintext
switchport trunk {allowed vlan vlan-list | native vlan {tag | vlan-id} | pruning vlan vlan-list}
no switchport trunk {allowed vlan | native vlan [tag] | pruning vlan}
```

#### Syntax Description

- **allowed vlan vlan-list** Sets the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the Usage Guidelines for the `vlan-list` choices.
- **native vlan vlan-id** Sets the native VLAN for sending and receiving untagged traffic when the interface is in IEEE 802.1Q trunking mode. The range is 1 to 4094.
- **native vlan tag** Enables native VLAN tagging on a particular trunk port.
- **pruning vlan vlan-list** Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the `vlan-list` choices.

#### Command Default

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

#### Command Modes

Interface configuration

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was modified. The keyword <code>native vlan tag</code> was added for Cisco Catalyst 9500 High Performance series of switches.</td>
</tr>
</tbody>
</table>

#### 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.
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.

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.

- **vlan dot1q tag native** global command needs to be enabled to execute the switchport trunk native vlan tag command.

- 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 enable native VLAN tagging on a trunk port:

```
Device> enable
Device(config)# interface HundredGigE 1/0/45
Device(config-if)# switchport trunk native vlan tag
```

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Device> enable
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> enable
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> enable
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.
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>dot1p</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Does not instruct the IP telephone about the voice VLAN. The telephone uses the configuration from the telephone key pad.</td>
</tr>
<tr>
<td><code>untagged</code></td>
<td>Configures the telephone to send untagged voice traffic. This is the default for the telephone.</td>
</tr>
<tr>
<td><code>name vlan_name</code></td>
<td>(Optional) Specifies the VLAN name to be used for voice traffic. You can enter up to 128 characters.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

When you enter a VLAN ID, the IP phone forwards voice traffic in IEEE 802.1Q frames, tagged with the specified VLAN ID. The device puts IEEE 802.1Q voice traffic in the voice VLAN.

When you select `dot1p`, `none`, or `untagged`, the device puts the indicated voice traffic in the access VLAN.

In all configurations, the voice traffic carries a Layer 2 IP precedence value. The default is 5 for voice traffic.

When you enable port security on an interface that is also configured with a voice VLAN, set the maximum allowed secure addresses on the port to 2. When the port is connected to a Cisco IP phone, the IP phone requires one MAC address. The Cisco IP phone address is learned on the voice VLAN, but not on the access VLAN. If you connect a single PC to the Cisco IP phone, no additional MAC addresses are required. If you connect more than one PC to the Cisco IP phone, you must configure enough secure addresses to allow one for each PC and one for the Cisco IP phone.
If any type of port security is enabled on the access VLAN, dynamic port security is automatically enabled on the voice VLAN.

You cannot configure static secure MAC addresses in the voice VLAN.

The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

This example show how to first populate the VLAN database by associating a VLAN ID with a VLAN name, and then configure the VLAN (using the name) on an interface, in the access mode:

You can also verify your configuration by entering the `show interfaces interface-id switchport` in privileged EXEC command and examining information in the Voice VLAN: row.

**Part 1 - Making the entry in the VLAN database:**

```bash
Device> enable
Device# configure terminal
Device(config)# vlan 55
Device(config-vlan)# name test
Device(config-vlan)# end
```

**Part 2 - Checking the VLAN database:**

```bash
Device> enable
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:**

```bash
Device> enable
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:**

```bash
Device> enable
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:**

```bash
Device> enable
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
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 | fast-hello error-reporting | message time message-timer-interval
        | recovery interval recovery-timer-interval}
no udld {aggressive | enable | message}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aggressive</code></td>
<td>Enables UDLD in aggressive mode on all fiber-optic interfaces.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td>Enables UDLD in normal mode on all fiber-optic interfaces.</td>
</tr>
<tr>
<td><code>fast-hello error-reporting</code></td>
<td>Reports link failure on the console instead of err-disabling the affected Fast UDLD port.</td>
</tr>
<tr>
<td><code>message time</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>recovery interval</code></td>
<td>Configures the error disable recovery timer value.</td>
</tr>
</tbody>
</table>

### Command Default

UDLD is disabled on all interfaces.

The message timer is set at 15 seconds.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
<td>The <code>fast-hello error-reporting</code> keyword was added to the command.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td></td>
<td>The <code>recovery interval</code> <code>recovery-timer-interval</code> keyword was introduced.</td>
</tr>
</tbody>
</table>

### 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 `Software Configuration Guide (Catalyst 9500 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> enable
Device# configure terminal
Device(config)# udld enable
```

You can verify your setting by entering the `show udld` command in privileged EXEC mode.
**udld fast-hello**

To enable Fast UniDirectional Link Detection (UDLD) on an individual interface which has UDLD configured on it, use the `udld fast-hello` command in interface configuration mode.

```
udld fast-hello message-timer-interval
```

**Syntax Description**

`message-timer-interval` Configures time in milliseconds between sending of messages in steady state. The range is from 200 to 1000 milliseconds.

**Command Default**

Fast UDLD is disabled by default.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

Fast UDLD enables detection of unidirectional links within the span of a few hundred milliseconds to a second. Fast UDLD runs on top of the UDLD process without interrupting it. To configure a port in Fast UDLD mode, it must first be configured in UDLD mode.

To enable Fast UDLD mode on a port, use the `udld fast-hello message-timer-interval` interface configuration command.

**Examples**

This example shows how to enable Fast UDLD on an port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld fast-hello 200
```

You can verify your settings by entering either the `show running-config` or the `show udld fast-hello interface` command in privileged EXEC mode.
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 command in global configuration mode, use the udld port command in interface configuration mode.

```
udld port [aggressive | disable]
no udld port [aggressive]
```

**Syntax Description**

- **aggressive** (Optional) Enables UDLD in aggressive mode on the specified interface.
- **disable** (Optional) Disables UDLD on the specified interface despite the global UDLD configuration.

**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 command in global configuration mode.

On nonfiber-optic interfaces, UDLD is disabled.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The disable keyword was introduced.</td>
</tr>
</tbody>
</table>

**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 command in interface configuration mode. To enable UDLD in aggressive mode, use the udld port aggressive command in interface configuration mode.

Use the udld port disable command on fiber-optic ports to return control of UDLD to the udld enable command in global configuration mode 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 command in global configuration mode. Use the udld port disable command on fiber-optic ports to remove this setting and to return control of UDLD enabling to the udld command in global configuration mode or to disable UDLD on nonfiber-optic ports.

You can use these commands to reset an interface shut down by UDLD:

- The udld reset command in privileged EXEC mode resets all interfaces shut down by UDLD.
- The shutdown and no shutdown command in interface configuration mode
• The **no udld enable** command in global configuration mode, followed by the **udld {aggressive | enable}** command in global configuration mode reenables UDLD globally.

• The **udld port disable** command in interface configuration mode, followed by the **udld port or udld port aggressive** command in interface configuration mode reenables UDLD on the specified interface.

• The **errdisable recovery cause udld** and **errdisable recovery interval interval** command in global configuration mode automatically recover from the UDLD error-disabled state.

This example shows how to enable UDLD on a port:

```
Device> enable
Device# configure terminal
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> enable
Device# configure terminal
Device(config)# interface gigabitethernet6/0/1
Device(config-if)# udld port disable
```

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

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# udld reset
1 ports shutdown by UDLD were reset.
```
vtp mode

To configure the VLAN Trunking Protocol (VTP) device mode, use the `vtp mode` command. To revert to the default server mode, use the `no` form of this command.

```
vtp mode { client | off | transparent }
novtp mode
```

### Syntax Description

- `client` Specifies the device as a client.
- `off` Specifies the device mode as off.
- `server` Specifies the device as a server.
- `transparent` Specifies the device mode as transparent.

### Command Default

Server.

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced</td>
</tr>
</tbody>
</table>

### Command Modes

Global configuration mode.

### Usage Guidelines

VLAN Trunking Protocol (VTP) is a Cisco Proprietary Layer 2 messaging protocol used to distribute the VLAN configuration information across multiple devices within a VTP domain. Without VTP, you must configure VLANs in each device in the network. Using VTP, you configure VLANs on a VTP server and then distribute the configuration to other VTP devices in the VTP domain.

In VTP transparent mode, you can configure VLANs (add, delete, or modify) and private VLANs. VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. The VTP configuration revision number is always set to zero (0). Transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP version 2.

A VTP device mode can be one of the following:

- `server` — You can create, modify, and delete VLANs and specify other configuration parameters, such as VTP version, for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the default mode.

  **Note** You can configure VLANs 1 to 1005. VLANs 1002 to 1005 are reserved for token ring in VTP version 2.

- `client` — VTP clients behave the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client.
• transparent — You can configure VLANs (add, delete, or modify) and private VLANs. VTP transparent
switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration
and does not synchronize its VLAN configuration based on received advertisements. Because of this,
the VTP configuration revision number is always set to zero (0). Transparent switches do forward VTP
advertisements that they receive out their trunk ports in VTP version 2.

• off — In the above three described modes, VTP advertisements are received and transmitted as soon as
the switch enters the management domain state. In the VTP off mode, switches behave the same as in
VTP transparent mode with the exception that VTP advertisements are not forwarded. You can use this
VTP device to monitor the VLANs.

\[\text{Note}\]

If you use the no vtp mode command to remove a VTP device, the device will
be configured as a VTP server. Use the vtp mode off command to remove a VTP
device.

**Example**

This example shows how to configure a VTP device in transparent mode and add VLANs 2, 3, and 4:

Device> enable
Device(config)# vtp mode transparent
Device(config)# vlan 2-4

**Example**

This example shows how to remove a device configured as a VTP device:

Device> enable
Device(config)# vtp mode off

**Example**

This example shows how to configure a VTP device as a VTP server and adds VLANs 2 and 3:

Device> enable
Device# vtp mode server
Device(config)# vlan 2,3

**Example**

This example shows how to configure a VTP device as a client:

Device> enable
Device# vtp mode client
PART VII

Multiprotocol Label Switching

• MPLS Commands, on page 793
MPLS Commands

- backup peer, on page 794
- encapsulation mpls, on page 795
- l2vpn xconnect context, on page 796
- load-balance, on page 797
- member pseudowire, on page 799
- mpls label range, on page 801
- mpls label protocol (interface configuration), on page 804
- mpls label protocol (global configuration), on page 805
- mpls ip (interface configuration), on page 806
- mpls ip (global configuration), on page 807
- mpls ip default-route, on page 808
- neighbor (MPLS), on page 809
- tunnel destination, on page 810
- tunnel mode gre multipoint, on page 811
- tunnel source, on page 812
- show ip pim mdt send, on page 814
- show ip pim mdt receive, on page 815
- show ip pim mdt history, on page 817
- show ip pim mdt bgp, on page 818
- ip pim sparse-mode, on page 819
- ip pim nbma-mode, on page 820
- mdt log-reuse, on page 821
- mdt default, on page 822
- mdt data, on page 824
- ip ospf network, on page 826
- ip multicast mrinfo-filter, on page 828
- ip multicast-routing, on page 829
- show mpls label range, on page 830
- show platform software fed switch l2vpn, on page 831
- show platform software fed switch mpls, on page 833
- show platform software l2vpn switch, on page 835
- xconnect, on page 837
backup peer

To specify a redundant peer for a pseudowire virtual circuit (VC), use the backup peer command in interface configuration mode or Xconnect configuration mode. To remove the redundant peer, use the no form of this command.

```
backup peer peer-router-ip-addr vcid [pw-class pw-class-name] [priority value]
```

```
no backup peer peer-router-ip-addr vcid
```

**Syntax Description**

- `peer-router-ip-addr`: IP address of the remote peer.
- `vcid`: 32-bit identifier of the VC between the devices at each end of the layer control channel.
- `pw-class`: (Optional) Specifies the pseudowire type. If this is not specified, the pseudowire type is inherited from the parent Xconnect.
- `pw-class-name`: (Optional) Name of the pseudowire that you created while establishing the pseudowire class.
- `priority value`: (Optional) Specifies the priority of the backup pseudowire in instances where multiple backup pseudowires exist. The range is from 1 to 10. The default is 1.

**Command Default**

No redundant peer is established.

**Command Modes**

Interface configuration (config-if)
Xconnect configuration (config-if-xconn)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The combination of the `peer-router-ip-addr` and `vcid` arguments must be unique on the device.

**Examples**

The following example shows how to configure a MPLS Xconnect with one redundant peer:

```
Device(config)# interface GigabitEthernet1/0/44
Device(config-if)# xconnect 10.0.0.1 100 encapsulation mpls
Device(config-if-xconn)# backup peer 10.0.0.2 200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xconnect</td>
<td>Binds an attachment circuit to a pseudowire for Xconnect service, and enters Xconnect configuration mode.</td>
</tr>
</tbody>
</table>
encapsulation mpls

To specify Multiprotocol Label Switching (MPLS) as the data encapsulation method, use the `encapsulation mpls` command in interface configuration mode. To remove the encapsulation type, use the `no` form of this command.

`encapsulation mpls
no encapsulation mpls`

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

**Command Default**
Enabled.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure MPLS as the data encapsulation method for a pseudowire interface:

```
Device> enable
Device# configure terminal
Device(config)# interface pseudowire 100
Device(config-if)# encapsulation mpls
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface pseudowire</td>
<td>Specifies the pseudowire interface.</td>
</tr>
<tr>
<td>xconnect</td>
<td>Binds an attachment circuit to a pseudowire for Xconnect service and enters Xconnect configuration mode.</td>
</tr>
</tbody>
</table>
To create a Layer 2 VPN (L2VPN) cross-connect context and enter Xconnect configuration mode, use the `l2vpn xconnect context` command in global configuration mode. To remove the connection, use the `no` form of this command.

```
l2vpn xconnect context context-name
no l2vpn xconnect context context-name
```

**Syntax Description**
```
context-name
Name of the cross connect context.
```

**Command Default**
L2VPN cross connections are not created.

**Command Modes**
Global configuration (config)

**Command History**
```
Release Modification
Cisco IOS XE Everest 16.6.1 This command was introduced.
```

**Usage Guidelines**
Use the `l2vpn xconnect context` command to define a cross-connect context that specifies the two members in Virtual Private Wire Service (VPWS), that is, attachment circuit to pseudowire, pseudo-to-pseudowire (multisegment pseudowire), or attachment circuit to attachment circuit (local connection). The type of members specified, that is, attachment circuit interface or pseudowire, automatically define the type of L2VPN service.

**Examples**
The following example shows how to establish an L2VPN cross-connect context:
```
Device> enable
Device# configure terminal
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# interworking ip
```

**Related Commands**
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interworking</td>
<td>Specifies the type of pseudowire and the type of traffic that can flow across the traffic.</td>
</tr>
</tbody>
</table>
```
load-balance

To set the load-distribution method for pseudowire, use the `load-balance` command in interface configuration mode. To reset the load-balancing mechanism to the default setting, use the `no` form of this command.

```
load-balance {flow | flow-label} {
  [ethernet [dst-mac | src-dst-mac | src-mac] | ip [dst-ip | src-dst-ip | src-ip]] |
  flow-label {both | receive | transmit} [static [advertise]]}
```

Syntax Description

**flow** Enables flow-based load balancing for pseudowire.

**ethernet** Specifies Ethernet pseudowire flow classification.

**dst-mac** Specifies load distribution based on the destination host MAC address.

**src-dst-mac** Specifies load distribution based on the source and destination host MAC address.

**src-mac** Specifies load distribution based on the source MAC address.

**ip** Specifies IP pseudowire flow classification.

**dst-ip** Specifies load distribution based on the destination host IP address.

**src-dst-ip** Specifies load distribution based on the source and destination host IP address.

**src-ip** Specifies load distribution based on the source host IP address.

**flow-label** Enables flow-aware transport of pseudowire.

**both** Enables flow-aware transport of pseudowire in both directions.

**receive** Enables flow-aware transport of pseudowire in the receiving direction.

**transmit** Enables flow-aware transport of pseudowire in the transmitting direction.

**static** Enables flow labels even if not signaled by the remote peer.

**advertise** Sends flow label sub type, length, value (sub-TLV).

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Examples

This example shows how to set flow-based load balancing for pseudowire in the context of a specified IP address:
Device> `enable`
Device# `configure terminal`
Device(config)# `interface pseudowire 17`
Device(config-if)# `load-balance flow ip 192.168.2.25`

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface pseudowire</code></td>
<td>Specifies the pseudowire interface.</td>
</tr>
</tbody>
</table>
**member pseudowire**

To specify a pseudowire interface that forms a Layer 2 VPN (L2VPN) cross connect, use the **member pseudowire** command in Xconnect configuration mode. To disconnect the pseudowire interface, use the **no** form of this command.

```
member pseudowire interface-number [ip-address vc-id {encapsulation mpls | template template-name}] [group group-name [priority number]]
```

**no member pseudowire interface-number**

**Syntax Description**

- **interface-number**: Interface number.
- **ip-address**: IP address of the peer.
- **vc-id**: The virtual circuit (VC) ID. The range is from 1 to 4294967295.
- **encapsulation mpls**: Specifies Multiprotocol Label Switching (MPLS) as the data encapsulation method.
- **template template-name**: (Optional) Specifies the template to be used for encapsulation and protocol configuration. The maximum size is 32 characters.
- **group group-name**: (Optional) Specifies the cross-connect member redundancy group name.
- **priority number**: (Optional) Specifies the cross-connect member priority. The range is from 0 to 16. The highest priority is 0. Lowest priority is 16.

**Command Default**

Devices that form an L2VPN cross connect are not specified.

**Command Modes**

Xconnect configuration (config-xconnect)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **member** command specifies the two members of the Virtual Private Wired Service (VPWS), multisegment pseudowire or local connect services. For VPWS, one member is an attachment circuit and the other member is a pseudowire interface. For a multisegment pseudowire, both members are pseudowire interfaces. For local connect, both members are active interfaces.

When both the pseudowire interface and the peer information are specified, an interface is dynamically created by using the **interface-number** argument specified in the **pseudowire** command.

Configure the group name to specify which of the two possible groups a member belongs to.

Configure a priority for each member so that the active members can be chosen based on priority when there are multiple redundant members. The default priority for a member is 0 (highest).

There can only be two groups, with a maximum of four members in one group and only one member in the other group (the lone member is for active redundancy and the other three are for backup redundancy). If a group name is not specified, only two members can be configured in the L2VPN cross-connect context.
The following example shows how to specify pseudowire as the attachment circuit type:

```
Device> enable
Device# configure terminal
Device(config)# l2vpn xconnect context con1
Device(config-xconnect)# member pseudowire 17
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>minimum-value</code></td>
<td>The value of the smallest label allowed in the label space. The default is 16.</td>
</tr>
<tr>
<td><code>maximum-value</code></td>
<td>The value of the largest label allowed in the label space. The default is platform-dependent.</td>
</tr>
<tr>
<td><code>static</code></td>
<td>(Optional) Reserves a block of local labels for static label assignments. If you omit the <code>static</code> keyword and the <code>minimum-static-value maximum-static-value</code> arguments, no labels are reserved for static assignment.</td>
</tr>
<tr>
<td><code>minimum-static-value</code></td>
<td>(Optional) The minimum value for static label assignments. There is no default value.</td>
</tr>
<tr>
<td><code>maximum-static-value</code></td>
<td>(Optional) The maximum value for static label assignments. There is no default value.</td>
</tr>
</tbody>
</table>

**Command Default**

The platform’s default values are used.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**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.

The following example displays the help lines when you configure the dynamic label with a minimum value of 16 and a maximum value of 100:

```
Device(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

The following example shows how to 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.

Device(config)# mpls label range 16 100 static ?
<16-100> static label value range

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.

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# mpls label range 200 4000
Device(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:

```
Device(config)# mpls label range 100 1000 static 16 99
Device(config)#
```

In the following output, the `show mpls label range` command, executed after a reload, shows that the configured range is now in effect:

```
Device# 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:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no mpls label range
Device(config)# end
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mpls label range</code></td>
<td>Displays the range of the MPLS local label space.</td>
</tr>
</tbody>
</table>
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**
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldp</td>
<td>Specifies that the label distribution protocol (LDP) is to be used on the interface.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config-if)# mpls label protocol ldp
```
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldp</td>
<td>Specifies that LDP is the default label distribution protocol.</td>
</tr>
</tbody>
</table>

**Command Default**

LDP is the default label distribution protocol.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config)# mpls label protocol ldp
```
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)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config)# configure terminal
Device(config-if)# interface TenGigabitEthernet1/0/3
Device(config-if)# mpls ip
```

The following example shows that label switching is enabled on the specified vlan interface (SVI) on a Cisco Catalyst switch:

```
Device(config)# configure terminal
Device(config-if)# interface vlan 1
Device(config-if)# mpls ip
```
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```
Device(config)# no mpls ip
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls ip (interface configuration)</td>
<td>Enables MPLS forwarding of IPv4 and IPv6 packets along normally routed paths for the associated interface.</td>
</tr>
</tbody>
</table>
**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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Device# configure terminal
Device(config)# mpls ip
Device(config)# mpls ip default-route
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls ip  (global configuration)</td>
<td>Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.</td>
</tr>
<tr>
<td>mpls ip  (interface configuration)</td>
<td>Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.</td>
</tr>
</tbody>
</table>
neighbor (MPLS)

To specify the peer IP address and virtual circuit (VC) ID value of a Layer 2 VPN (L2VPN) pseudowire, use the `neighbor` command in interface configuration mode. To remove the peer IP address and VC ID value of an L2VPN pseudowire, use the `no` form of this command.

```
neighbor peer-address vcid-value
no neighbor
```

**Syntax Description**

- `peer-address`  IP address of the provider edge (PE) peer.
- `vcid-value`  VC ID value. The range is from 1 to 4294967295.

**Command Default**

Peer address and VC ID value of a pseudowire are not specified.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must configure the `neighbor` command for the pseudowire to be functional.

**Examples**

The following example shows how to specify a peer IP address of 10.1.2.3 and a VC ID value of 100.

```
Device> enable
Device# configure terminal
Device(config)# interface pseudowire 100
Device(config-if)# neighbor 10.1.2.3 100
```
tunnel destination

To specify the destination for a tunnel interface, use the `tunnel destination` command in interface configuration mode. To remove the destination, use the `no` form of this command.

```
tunnel destination {host-name ip-address ipv6-address | dynamic}
```

**Syntax Description**

- `host-name` Name of the host destination.
- `ip-address` IP address of the host destination expressed in dotted decimal notation.
- `ipv6-address` IPv6 address of the host destination expressed in IPv6 address format.
- `dynamic` Applies the tunnel destination address dynamically to the tunnel interface.

**Command Default**

No tunnel interface destination is specified.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination addresses. The workaround is to create a loopback interface and configure the packet source off of the loopback interface.

**Examples**

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in a global or non-VRF environment:

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface tunnel 2 in a VRF environment. Use the `vrf definition vrf-name` and the `vrf forwarding vrf-name` commands to configure and apply VRF.

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```
**tunnel mode gre multipoint**

To set the global encapsulation mode on all roaming interfaces of a mobile device to multipoint generic routing encapsulation (GRE), use the `tunnel mode gre multipoint` command in mobile device configuration mode. To restore the global default encapsulation mode, use the `no` form of this command.

```
tunnel mode gre multipoint
no tunnel mode gre multipoint
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The default encapsulation mode for Mobile IP is IP-in-IP encapsulation.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to configure multipoint GRE as the tunnel mode.

The `no tunnel mode gre multipoint` command instructs the mobile device to revert to the default and register with IP-in-IP encapsulation.

**Examples**

The following example configures multipoint GRE as the tunnel mode:

```
Device(config-if)# tunnel mode gre multipoint
```
tunnel source

To set the source address for a tunnel interface, use the `tunnel source` command in interface configuration mode. To remove the source address, use the `no` form of this command.

```
tunnel source {ip-address | ipv6-address | interface-type interface-number | dynamic}

no tunnel source
```

**Syntax Description**

- `ip-address`: Source IP address of the packets in the tunnel.
- `ipv6-address`: Source IPv6 address of the packets in the tunnel.
- `interface-type`: Interface type.
- `interface-number`: Port, connector, or interface card number. The numbers are assigned at the factory at the time of installation or when added to a system. This number can be displayed with the `show interfaces` command.
- `dynamic`: Applies the tunnel source address dynamically to the tunnel interface.

**Command Default**

No tunnel interface source address is set.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The source address is either an explicitly defined IP address or the IP address assigned to specified interface. You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination addresses. The workaround is to create a loopback interface and source packets from the loopback interface.

**Examples**

The following example shows how to configure the logical Layer 3 GRE tunnel interface interface tunnel 2 in a global or non-VRF environment:

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
```

The following example shows how to configure the logical Layer 3 GRE tunnel interface interface tunnel 2 in a VRF environment. Use the `vrf definition vrf-name` and the `vrf forwarding vrf-name` commands to configure and apply VRF.

```
Device> enable
Device# configure terminal
Device(config)# interface tunnel 2
Device(config-if)# ip address 100.1.1.1 255.255.255.0
```
Device(config-if)# tunnel source 10.10.10.1
Device(config-if)# tunnel destination 10.10.10.2
Device(config-if)# tunnel mode gre ip
Device(config-if)# end
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**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Displays the data MDT groups in use by the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 96: show ip pim mdt send Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source, group</td>
<td>Source and group addresses that this router has switched over to data MDTs.</td>
</tr>
<tr>
<td>MDT-data group</td>
<td>Multicast address over which these data MDTs are being sent.</td>
</tr>
<tr>
<td>ref_count</td>
<td>Number of (S, G) pairs that are reusing this data MDT.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf</td>
<td>Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Provides a detailed description of the data MDT advertisements received.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 97: show ip pim mdt receive Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group:172.16.8.0</td>
<td>Group that caused the data MDT to be built.</td>
</tr>
<tr>
<td>source:10.0.0.100</td>
<td>VRF source that caused the data MDT to be built.</td>
</tr>
<tr>
<td>ref_count:13</td>
<td>Number of (S, G) pairs that are reusing this data MDT.</td>
</tr>
<tr>
<td>OIF count:1</td>
<td>Number of interfaces out of which this multicast data is being forwarded.</td>
</tr>
</tbody>
</table>
## show ip pim mdt receive

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flags:</td>
<td>Information about the entry.</td>
</tr>
<tr>
<td>• A--</td>
<td>candidate Multicast Source Discovery Protocol (MSDP) advertisement</td>
</tr>
<tr>
<td>• B--</td>
<td>bidirectional group</td>
</tr>
<tr>
<td>• D--</td>
<td>dense</td>
</tr>
<tr>
<td>• C--</td>
<td>connected</td>
</tr>
<tr>
<td>• F--</td>
<td>register flag</td>
</tr>
<tr>
<td>• I--</td>
<td>received source-specific host report</td>
</tr>
<tr>
<td>• J--</td>
<td>join shortest path source tree (SPT)</td>
</tr>
<tr>
<td>• L--</td>
<td>local</td>
</tr>
<tr>
<td>• M--</td>
<td>MSDP created entry</td>
</tr>
<tr>
<td>• P--</td>
<td>pruned</td>
</tr>
<tr>
<td>• R--</td>
<td>RP bit set</td>
</tr>
<tr>
<td>• S--</td>
<td>sparse</td>
</tr>
<tr>
<td>• s--</td>
<td>Source Specific Multicast (SSM) group</td>
</tr>
<tr>
<td>• T--</td>
<td>SPT bit set</td>
</tr>
<tr>
<td>• X--</td>
<td>proxy join timer running</td>
</tr>
<tr>
<td>• U--</td>
<td>URL Rendezvous Directory (URD)</td>
</tr>
<tr>
<td>• Y--</td>
<td>joined MDT data group</td>
</tr>
<tr>
<td>• y--</td>
<td>sending to MDT data group</td>
</tr>
<tr>
<td>• Z--</td>
<td>multicast tunnel</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
<tr>
<td>interval minutes</td>
<td>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).</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDT-data group</td>
<td>The MDT data group for which information is being shown.</td>
</tr>
<tr>
<td>Number of reuse</td>
<td>The number of data MDTs that have been reused in this group.</td>
</tr>
</tbody>
</table>
**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.

```plaintext
show ip pim [vrf vrf-name] mdt bgp
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(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 <code>vrf-name</code> argument.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
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 99: show ip pim mdt bgp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MDT-default group</td>
<td>The MDT default groups that have been advertised to this router.</td>
</tr>
<tr>
<td>rid:10.1.1.1</td>
<td>The BGP router ID of the advertising router.</td>
</tr>
<tr>
<td>next_hop:10.1.1.1</td>
<td>The BGP next hop address that was contained in the advertisement.</td>
</tr>
</tbody>
</table>
ip pim sparse-mode

To configure a multiaccess WAN interface to be in sparse mode, use the `ip pim sparse-mode` command in interface configuration mode. To disable this function, use the `no` form of this command.

```
ip pim sparse-mode
no ip pim sparse-mode
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The command is disabled.

**Command Modes**

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When this command is configured on all interfaces, any existing groups running in sparse mode will continue to operate in sparse mode but will use an RP address set to 0.0.0.0. Multicast entries with an RP address set to 0.0.0.0 will exhibit the following behavior:

- Existing (S, G) states will be maintained.
- No PIM Join or Prune messages for (*. G) or (S, G, RPbit) are sent.
- Received (*. G) or (S, G, RPbit) Joins or Prune messages are ignored.
- No registers are sent and traffic at the first hop is dropped.
- Received registers are answered with register stop.
- Asserts are unchanged.
- The (*. G) outgoing interface list (olist) is maintained only for the Internet Group Management Protocol (IGMP) state.
- Multicast Source Discovery Protocol (MSDP) source active (SA) messages for RP 0.0.0.0 groups are still accepted and forwarded.

**Examples**

The following example configures an interface to be in sparse mode:

```
Device(config-if)# ip pim sparse-mode
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim</td>
<td>Enables PIM on an interface.</td>
</tr>
</tbody>
</table>
ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast multiaccess (NBMA) mode, use the `ip pim nbma-mode` command in interface configuration mode. To disable this function, use the `no` form of this command.

```
ip pim nbma-mode
no ip pim nbma-mode
```

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

**Command Default**
The command is disabled.

**Command Modes**
Interface configuration (config-if)
Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command on Frame Relay, Switched Multimegabit Data Service (SMDS), or ATM only, especially when these media do not have native multicast available. Do not use this command on multicast-capable LANs such as Ethernet or FDDI.

When this command is configured, each Protocol Independent Multicast (PIM) join message is tracked in the outgoing interface list of a multicast routing table entry. Therefore, only PIM WAN neighbors that have joined for the group will get packets sent as data-link unicasts. This command should only be used when the `ip pim sparse-mode` command is configured on the interface. This command is not recommended for LANs that have natural multicast capabilities.

**Examples**
The following example configures an interface to be in NBMA mode:

```
Device(config-if)# ip pim nbma-mode
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip pim</td>
<td>Enables PIM on an interface.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdt data</td>
<td>Configures the multicast group address range for data MDT groups.</td>
</tr>
<tr>
<td>mdt default</td>
<td>Configures a default MDT group for a VPN VRF.</td>
</tr>
</tbody>
</table>
**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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-address</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command Default**
The command is disabled.

**Command Modes**
- VRF address family configuration (config-vrf-af)
- VRF configuration (config-vrf)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdt data</td>
<td>Configures the multicast group address range for data MDT groups.</td>
</tr>
</tbody>
</table>
**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.

```plaintext
mdt data threshold kb/s
no mdt data threshold kb/s
```

**Syntax Description**

- `threshold kb/s` (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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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 vrfl accept-rp auto-rp
!

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>mdt default</td>
<td>Configures a default MDT group for a VPN VRF.</td>
</tr>
</tbody>
</table>
ip ospf network

To configure the Open Shortest Path First (OSPF) network type to a type other than the default for a given medium, use the `ip ospf network` command in interface configuration mode. To return to the default value, use the `no` form of this command.

```
ip ospf network {broadcast | non-broadcast | [point-to-multipoint [non-broadcast] | point-to-point]}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>broadcast</code></td>
<td>Sets the network type to broadcast.</td>
</tr>
<tr>
<td><code>non-broadcast</code></td>
<td>Sets the network type to nonbroadcast multiaccess (NBMA).</td>
</tr>
<tr>
<td><code>point-to-multipoint</code></td>
<td>Sets the network type to point-to-multipoint. The optional <code>non-broadcast</code> keyword sets the point-to-multipoint network to be nonbroadcast. If you use the <code>non-broadcast</code> keyword, the <code>neighbor</code> command is required.</td>
</tr>
<tr>
<td><code>point-to-point</code></td>
<td>Sets the network type to point-to-point.</td>
</tr>
</tbody>
</table>

### Command Default

Depends on the network type.

### Command Modes

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration (config-if)</td>
</tr>
<tr>
<td>Virtual network interface (config-if-vnet)</td>
</tr>
</tbody>
</table>

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Using this feature, you can configure broadcast networks as NBMA networks when, for example, routers in your network do not support multicast addressing. You can also configure nonbroadcast multiaccess networks (such as X.25, Frame Relay, and Switched Multimegabit Data Service (SMDS)) as broadcast networks. This feature saves you from needing to configure neighbors.

Configuring NBMA networks as either broadcast or nonbroadcast assumes that there are virtual circuits from every router to every router or fully meshed networks. However, there are other configurations where this assumption is not true. For example, a partially meshed network. In these cases, you can configure the OSPF network type as a point-to-multipoint network. Routing between two routers that are not directly connected will go through the router that has virtual circuits to both routers. You need not configure neighbors when using this feature.

If this command is issued on an interface that does not allow it, this command will be ignored.

OSPF has two features related to point-to-multipoint networks. One feature applies to broadcast networks; the other feature applies to nonbroadcast networks:

- **On point-to-multipoint, broadcast networks**, you can use the `neighbor` command, and you must specify a cost to that neighbor.
- **On point-to-multipoint, nonbroadcast networks**, you must use the `neighbor` command to identify neighbors. Assigning a cost to a neighbor is optional.
Examples

The following example sets your OSPF network as a broadcast network:

```
Device(config)# interface serial 0
Device(config-if)# ip address 192.168.77.17 255.255.255.0
Device(config-if)# ip ospf network broadcast
Device(config-if)# encapsulation frame-relay
```

The following example illustrates a point-to-multipoint network with broadcast:

```
Device(config)# interface serial 0
Device(config-if)# ip address 10.0.1.1 255.255.255.0
Device(config-if)# encapsulation frame-relay
Device(config-if)# ip ospf cost 100
Device(config-if)# ip ospf network point-to-multipoint
Device(config-if)# frame-relay map ip 10.0.1.3 202 broadcast
Device(config-if)# frame-relay map ip 10.0.1.4 203 broadcast
Device(config-if)# frame-relay map ip 10.0.1.5 204 broadcast
Device(config-if)# frame-relay local-dlci 200

Device(config-if)# router ospf 1
Device(config-if)# network 10.0.1.0 0.0.0.255 area 0
Device(config-if)# neighbor 10.0.1.5 cost 5
Device(config-if)# neighbor 10.0.1.4 cost 10
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frame-relay map</td>
<td>Defines mapping between a destination protocol address and the DLCI used to connect to the destination address.</td>
</tr>
<tr>
<td>neighbor (OSPF)</td>
<td>Configures OSPF routers interconnecting to nonbroadcast networks.</td>
</tr>
<tr>
<td>x25 map</td>
<td>Sets up the LAN protocols-to-remote host mapping.</td>
</tr>
</tbody>
</table>
ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter** command in global configuration mode. To remove the filter on mrinfo requests, use the **no** form of this command.

```
ip multicast [vrf vrf-name] mrinfo-filter access-list
no ip multicast [vrf vrf-name] mrinfo-filter
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vr</td>
<td>(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>vrf-name</td>
<td>(Optional) Name assigned to the VRF.</td>
</tr>
<tr>
<td>access-list</td>
<td>IP standard numbered or named access list that determines which networks or hosts can query the local multicast device with the mrinfo command.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The **ip multicast mrinfo-filter** command filters the mrinfo 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 mrinfo requests are filtered. mrinfo requests from any sources permitted by the ACL are allowed to proceed.

**Examples**

The following example shows how to filter mrinfo request packets from all hosts on network 192.168.1.1 while allowing requests from any other hosts:

```
ip multicast mrinfo-filter 51
access-list 51 deny 192.168.1.1
access list 51 permit any
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mrinfo</td>
<td>Queries a multicast device about which neighboring multicast devices are peering with it.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[vrf vrf-name]</code></td>
<td>(Optional) Enables IP multicast routing for the Multicast VPN routing and forwarding (MVRF) instance specified for the <code>vrf-name</code> argument.</td>
</tr>
</tbody>
</table>

**Command Default**

IP multicast routing is disabled.

**Command Modes**

Global configuration (config).

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Device(config)# ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Device(config)# no ip multicast-routing
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip pim</code></td>
<td>Enables PIM on an interface.</td>
</tr>
</tbody>
</table>
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.

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

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:

```
Device# show mpls label range
Downstream label pool: Min/Max label: 16/100
Device# configure terminal
Device(config)# mpls label range 101 4000
Device(config)# exit
Device# show mpls label range
Downstream label pool: Min/Max label: 101/4000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpls label range</td>
<td>Configures a range of values for use as local labels.</td>
</tr>
</tbody>
</table>
show platform software fed switch l2vpn

To display device-specific software information, use the `show platform software fed switch` command.

```
show platform software fed switch {switch number | active | standby} l2vpn {atom-disposition | atom-imposition | summary | vfi-segment | xconnect}
```

**Note**

This topic elaborates on only the Layer 2 VPN-specific (L2VPN-specific) options available with the `show platform software fed switch l2vpn` command.

**Syntax Description**

<table>
<thead>
<tr>
<th>switch {switch number</th>
<th>active</th>
<th>standby}</th>
<th>Specifies the device for which you want to display information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• switch number: Enter the switch ID. Displays information about the specified switch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• active: Displays information about the active switch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• standby: Displays information about the standby switch, if available.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**l2vpn**

Displays L2VPN information. Choose one of the following options:

| • atom-disposition: Displays L2VPN atom disposition information. |
| • atom-imposition: Displays L2VPN atom imposition information. |
| • summary: Displays L2VPN summary. |
| • vfi-segment: Displays L2VPN Virtual Forwarder Interface (VFI) segment information. |
| • xconnect: Displays L2VPN Xconnect information. |

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output of the `show platform software fed switch l2vpn` command:

```
Device# show platform software fed switch 1 l2vpn atom-disposition all

Number of disp entries:25
ATOM_DISP:6682 ac_ifhdl:4325527 xconid:0 dot1q_etype:0
disp_flags:0x111 pdflags:0 hw_handle:0x4b010118
disp_flags (FED) in detail CW_IN_USE VCCV L2L
AAL: id:1258357016 , port_id:4325527, adj_flags:0x4 pw_id:1074 ref_cnt:1
adj_flags in detail: PORT MODE VC CW Enabled
```
show platform software fed switch l2vpn

```
port_hdl:0x5c01020f, dot1q:0 , is_vfi_seg;1 vfi_seg_hdl:0 stats_valid:1
drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6c6e6458(18438) di_id:23713 rih:0x7f1c6ce845a8(5154)
ATOM_DISP:1265 ac_ifhdl:311 xconid:1104 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2902458681 , port_id:311, adj_flags:0xc pw_id:991 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8a01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b5078(17152) di_id:24265 rih:0x7f1c6664ac8(3678)
ATOM_DISP:17319 ac_ifhdl:1248 xconid:3500 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2348810629 , port_id:1248, adj_flags:0xc pw_id:993 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8c01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b17288(16884) di_id:24265 rih:0x7f1c6a6b4ac8(3678)
ATOM_DISP:17335 ac_ifhdl:1250 xconid:3201 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:370765124 , port_id:1249, adj_flags:0xc pw_id:991 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8a01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6664ac8(17152) di_id:24265 rih:0x7f1c6664ac8(3678)
ATOM_DISP:17325 ac_ifhdl:1249 xconid:3201 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2348810629 , port_id:1248, adj_flags:0xc pw_id:993 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8c01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b17288(16884) di_id:24265 rih:0x7f1c6a6b4ac8(3678)
ATOM_DISP:17335 ac_ifhdl:1250 xconid:3202 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2348810629 , port_id:1248, adj_flags:0xc pw_id:993 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8c01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b17288(16884) di_id:24265 rih:0x7f1c6a6b4ac8(3678)
ATOM_DISP:17335 ac_ifhdl:1250 xconid:3202 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2348810629 , port_id:1248, adj_flags:0xc pw_id:993 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8c01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b17288(16884) di_id:24265 rih:0x7f1c6a6b4ac8(3678)
ATOM_DISP:17335 ac_ifhdl:1250 xconid:3202 dot1q_etype:0
disp_flags (FED) in detail CW_IN_USE VCCV ETHERNET_ITW
AAL: id:2348810629 , port_id:1248, adj_flags:0xc pw_id:993 ref_cnt:1
  adj_flags in detail: TYPE5 VC CW Enabled
  port_hdl:0x8c01001f, dot1q:0 , is_vfi_seg;0 vfi_seg_hdl:0 stats_valid:1
  drop_adj_flag:0 unsupported_feature:0
sih:0x7f1c6a6b17288(16884) di_id:24265 rih:0x7f1c6a6b4ac8(3678)
```

show platform software fed switch mpls

To display device-specific software information, use the show platform software fed switch command.

```
show platform software fed switch {switch number | active | standby} mpls {eos | forwarding | label_oce | lookup | summary}
```

**Note**
This topic elaborates only the MPLS-specific options available with the show platform software fed switch mpls command.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Specifying the device for which you want to display information.</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch {switch number</td>
<td>active</td>
</tr>
<tr>
<td>mpls</td>
<td>Displays MPLS information. Choose one of the following options:</td>
</tr>
<tr>
<td>eos</td>
<td>Displays MPLS end of stack (EOS) information.</td>
</tr>
<tr>
<td>forwarding</td>
<td>Displays MPLS forwarding information.</td>
</tr>
<tr>
<td>label_oce</td>
<td>Displays MPLS label output chain element (OCE) information.</td>
</tr>
<tr>
<td>lookup</td>
<td>Displays MPLS lookup information.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays the summary of the MPLS configuration.</td>
</tr>
</tbody>
</table>

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output of the show platform software fed switch mpls command:

```
Device# show platform software fed switch 1 mpls summary
Number of lentries: 2024
  # of create/modify/delete msgs: 3595/15390/1571
  LENTRY create paused: 0
  LENTRY Number of create paused: 0
  LENTRY Number of add after create paused: 3595
  LENTRY Number of out-of-resource: 0
```
Number of label oce entries: 4015
  # of create/modify/delete msgs: 21165/2993/17150
  # of unsupported_recursiveLbls: 0
  # of AAL mpls adj deleted and recreated: 0
  # of AAL local mpls adj deleted and recreated: 0
  # of changes from mpls-adj -> mpls-local-adj: 0
  # of changes from local-mpls-adj -> mpls-adj: 0
  # of out label changes in lbloce: 0
  # of collapsed oce: 0
  # of unsupported_nh: 0

Number of EOS oce entries: 1991
  # of create/modify/delete msgs: 6303/7/4312
  Number of ECR bwalk apply skipped: 0

Number of ECR entries: ipv4/ipv6: 22/0
  # of create/modify/delete msgs: 5196/1/5174
  # of ECR nested backwalks ignore: 0
  ECR OOR Retry queue size: 0

AAL L3 ECR summary:
  # of ecr add/modify/delete: 6/4/3
  # of modify from level-1 to level-2: 0
  # of modify from level-2 to level-1: 0
  # of ecr delete errs: 0
  # of ecr create skip refcnt: 0
  # of ecr modify inuse: 1 nochange: 3 inplace: 0

MPLS Summary: Info at AAL layers:
General info:
  Number of Physical ASICs: 2
  Number of ASIC Instances: 4
  num_modify_stack_in_use: 0
  num_modify_ri_in_use: 0
  Feature IDs: {l2_fid: 57 mpls_fid: 152 vpws_fid: 153 vpls_fid: 154}
MAX values from selected SDM template:
  MAX label entries: 45056
  MAX LSPA entries: 32768
  MAX L3VPN VRF(rc:0): 1024
  MAX L3VPN Routes PerVRF Mode(rc:0): 209920
  MAX L3VPN Routes PerPrefix Mode(rc:0): 32768
  MAX ADJ stats counters: 49152
Resource sharing info:
  SI: 1133/131072
  RI: 4943/98304
  Well Known Index: 8024/2048
  Tcam: 4962/245760
  lv1_ecr: 0/64
  lv2_ecr: 3/256
  lspa: 0/32769
  label_stack_id: 26/65537

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show platform software l2vpn switch

To display software information of Layer 2 VPN (L2VPN), use the `show platform software l2vpn switch` command.

```
show platform software fed switch {switch number | active | standby} {F0 | F1 | R0 | R1 | RP | {active | standby}} {atom | disposition | imposition | internal}
```

**Syntax Description**

- **switch** `switch number | active | standby`: The device for which you want to display information.
  - `switch number`: Switch ID. Displays information for the specified switch.
  - `active`: Displays information for the active switch.
  - `standby`: Displays information for the standby switch, if available.

- **F0**: Displays information about the Embedded Service Processor (ESP) slot 0.
- **F1**: Displays information about the ESP slot 1.
- **R0**: Displays information about the Route Processor (RP) slot 0.
- **R1**: Displays information about the RP slot 1.
- **RP**: Displays information about the RP. Choose one of the following options:
  - `active`: Displays information about the active RP.
  - `standby`: Displays information about the standby RP.
- **atom**: Displays information about the Any Transport over MPLS (AToM) cross-connect table.
- **disposition**: Displays information about the disposition output chain element (OCE).
- **imposition**: Displays information about the imposition OCE.
- **internal**: Displays AToM internal state and statistics.

**Command Modes**

- User EXEC (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output of the `show platform software l2vpn switch` command:

```
Device# show platform software l2vpn switch 1 R0 atom
```
Number of xconnect entries: 24

AToM Cross-Connect xid 0x137, ifnumber 0x137
   AC VLAN(IW:ETHERNET) -> Imp 0x316d(ATOM_IMP), OM handle: 0x3480fb3268
   VLAN Info: outVlan id: 1104, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e0, ifnumber 0x4e0
   AC VLAN(IW:ETHERNET) -> Imp 0x348118f120
   VLAN Info: outVlan id: 3500, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e1, ifnumber 0x4e1
   AC VLAN(IW:ETHERNET) -> Imp 0x348118f348
   VLAN Info: outVlan id: 3201, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e1, ifnumber 0x4e1
   AC VLAN(IW:ETHERNET) -> Imp 0x348118f570
   VLAN Info: outVlan id: 3201, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e2, ifnumber 0x4e2
   AC VLAN(IW:VLAN) -> Imp 0x348118f798
   VLAN Info: outVlan id: 3202, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e2, ifnumber 0x4e2
   AC VLAN(IW:VLAN) -> Imp 0x348118f9c0
   VLAN Info: outVlan id: 3203, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e3, ifnumber 0x4e3
   AC VLAN(IW:VLAN) -> Imp 0x348118fbed8
   VLAN Info: outVlan id: 3203, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e3, ifnumber 0x4e3
   AC VLAN(IW:VLAN) -> Imp 0x348118fe10
   VLAN Info: outVlan id: 3203, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

AToM Cross-Connect xid 0x4e4, ifnumber 0x4e4
   AC VLAN(IW:ETHERNET) -> Imp 0x3481189e20
   VLAN Info: outVlan id: 3204, inVlan id: 0, outEther: 0x8100, peerVlan id: 0, dot1qAny: 0

...
xconnect

To bind an attachment circuit to a pseudowire, and to configure an Any Transport over MPLS (AToM) static pseudowire, use the `xconnect` command in interface configuration mode. To restore the default values, use the `no` form of this command.

```
xconnect peer-ip-address vc-id encapsulation mpls [pw-type]
```

```
o xconnect peer-ip-address vc-id encapsulation mpls [pw-type]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer-ip-address</td>
<td>IP address of the remote provider edge (PE) peer. The remote router ID can be any IP address, as long as it is reachable.</td>
</tr>
<tr>
<td>vc-id</td>
<td>The 32-bit identifier of the virtual circuit (VC) between PE devices.</td>
</tr>
<tr>
<td>encapsulation mpls</td>
<td>Specifies Multiprotocol Label Switching (MPLS) as the tunneling method.</td>
</tr>
<tr>
<td>pw-type</td>
<td>(Optional) Pseudowire type. You can specify one of the following types:</td>
</tr>
<tr>
<td></td>
<td>• 4: Specifies Ethernet VLAN.</td>
</tr>
<tr>
<td></td>
<td>• 5: Specifies Ethernet port.</td>
</tr>
</tbody>
</table>

**Command Default**

The attachment circuit is not bound to the pseudowire.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The use of the `xconnect` command and the interface configuration mode `bridge-group` commands is not supported on the same physical interface.

The combination of the `peer-ip-address` and `vcid` arguments must be unique on the device. Each Xconnect configuration must have a unique combination of `peer-ip-address` and `vcid` configuration.

The same `vcid` value that identifies the attachment circuit must be configured using the `xconnect` command on the local and remote PE device. The VC ID creates the binding between a pseudowire and an attachment circuit.

**Examples**

The following example shows how to enter Xconnect configuration mode and bind the attachment circuit to a pseudowire VC:

```
Device# configure terminal
Device(config)# interface TenGigabitEthernet1/0/36
Device(config-if)# no ip address
Device(config-if)# xconnect 10.1.10.1 962 encapsulation mpls
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>encapsulation mpls</code></td>
<td>Specifies MPLS as the data encapsulation method.</td>
</tr>
</tbody>
</table>
PART VIII

Network Management

• Network Management Commands, on page 841
Network Management Commands

- description (ERSPAN), on page 843
- destination (ERSPAN), on page 844
- erspan-id, on page 846
- filter (ERSPAN), on page 847
- header-type, on page 849
- ip dscp (ERSPAN), on page 850
- ip ttl (ERSPAN), on page 851
- ip wccp, on page 852
- map platform-type, on page 854
- match platform-type, on page 855
- monitor capture (interface/control plane), on page 856
- monitor capture buffer, on page 858
- monitor capture clear, on page 859
- monitor capture export, on page 860
- monitor capture file, on page 861
- monitor capture limit, on page 863
- monitor capture match, on page 864
- monitor capture start, on page 865
- monitor capture stop, on page 866
- monitor session, on page 867
- monitor session destination, on page 869
- monitor session filter, on page 873
- monitor session source, on page 875
- monitor session type, on page 877
- mtu (ERSPAN), on page 879
- origin, on page 880
- show capability feature monitor, on page 882
- show class-map type control subscriber, on page 883
- show ip sla statistics, on page 884
- show monitor, on page 886
- show monitor capture, on page 888
- show monitor session, on page 890
- show parameter-map type subscriber attribute-to-service, on page 893
• show platform software fed switch ip wccp, on page 894
• show platform software swspan, on page 896
• snmp ifmib ifindex persist, on page 898
• snmp-server enable traps, on page 899
• snmp-server enable traps bridge, on page 902
• snmp-server enable traps bulkstat, on page 903
• snmp-server enable traps call-home, on page 904
• snmp-server enable traps cef, on page 905
• snmp-server enable traps cpu, on page 906
• snmp-server enable traps envmon, on page 907
• snmp-server enable traps errdisable, on page 908
• snmp-server enable traps flash, on page 909
• snmp-server enable traps isis, on page 910
• snmp-server enable traps license, on page 911
• snmp-server enable traps mac-notification, on page 912
• snmp-server enable traps ospf, on page 913
• snmp-server enable traps pim, on page 914
• snmp-server enable traps port-security, on page 915
• snmp-server enable traps power-ethernet, on page 916
• snmp-server enable traps snmp, on page 917
• snmp-server enable traps storm-control, on page 918
• snmp-server enable traps stpx, on page 919
• snmp-server enable traps transceiver, on page 920
• snmp-server enable traps vrfmib, on page 921
• snmp-server enable traps vstack, on page 922
• snmp-server engineID, on page 923
• snmp-server group, on page 924
• snmp-server host, on page 928
• snmp-server user, on page 933
• snmp-server view, on page 937
• source (ERSPAN), on page 939
• switchport mode access, on page 940
• switchport voice vlan, on page 941
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `description` argument can be up to 240 characters.

**Examples**

The following example shows how to describe an ERSPAN source session:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# description source1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>monitor session type</code></td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip address 10.1.1.1
Device(config-mon-erspan-src-dst)#
```

The following sample output from the `show monitor session all` displays different IP addresses for source session destinations:

```
Device# show monitor session all

Session 1
--------
Type : ERSPAN Source Session
Status : Admin Disabled

Session 2
--------
Type : ERSPAN Source Session
Status : Admin Disabled
```
Source VLANs : RX Only : 400
Destination IP Address : 10.1.1.1
Destination ERSPAN ID : 220
Origin IP Address : 192.0.2.1
IP TTL : 10
ERSPAN header-type : 3

Session 3
---------
Type : ERSpan Source Session
Status : Admin Enabled
Source Ports :
Both : Fo1/0/2
Destination IP Address : 10.1.1.2
Destination ERSPAN ID : 251
Origin IP Address : 192.0.2.2
ERSPAN header-type : 3

Session 4
---------
Type : ERSpan Source Session
Status : Admin Disabled
Source VLANs :
Both : 30
Destination IP Address : 10.1.1.3
Destination ERSPAN ID : 260
Origin IP Address : 192.0.2.3

Session 5
---------
Type : ERSpan Source Session
Status : Admin Enabled
Source VLANs :
Both : 500
Destination IP Address : 10.1.1.4
Destination ERSPAN ID : 100
Origin IP Address : 192.0.2.4

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>erspan-id</td>
<td>Configures the ID used by the destination session to identify the ERSpan traffic.</td>
</tr>
<tr>
<td>ip ttl</td>
<td>Configures TTL values for packets in the ERSpan traffic.</td>
</tr>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSpan source or destination session.</td>
</tr>
<tr>
<td>origin</td>
<td>Configures an IP address used as the source of the ERSpan traffic.</td>
</tr>
</tbody>
</table>
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**

- `erspan-id`  
  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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure an ERSPAN ID for a destination session:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# erspan-id 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Configures an ERSPAN destination session and specifies destination properties.</td>
</tr>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
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 | sgt sgt-id [{} | {}] | vlan vlan-id [{} | {}]}
no filter {ip [{access-group} | {standard-access-list extended-access-list acl-name}] | ipv6 [{access-group} | mac [{access-group}] | sgt sgt-id [{} | {}] | vlan vlan-id [{} | {}]}
```

Syntax Description

- **ip** Specifies the IP access control rules.
- **access-group** Specifies an access control group.
- **standard-access-list** Standard IP access list.
- **extended-access-list** Extended IP access list.
- **acl-name** Access list name.
- **ipv6** Specifies the IPv6 access control rules.
- **mac** Specifies the media access control (MAC) rules.
- **sgt** sgt-ID Specifies the Security Group Tag (SGT). Valid values are from 1 to 65535.
- **vlan** vlan-ID Specifies the ERSpan source VLAN. Valid values are from 1 to 4094.

Command Default

Source VLAN filtering is not configured.

Command Modes

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The sgt keyword was introduced.</td>
</tr>
<tr>
<td></td>
<td>This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>The sgt keyword was introduced.</td>
</tr>
<tr>
<td></td>
<td>This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

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:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# filter vlan 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
header-type

To configure the ERSPAN header type for encapsulation, use the `header-type` command in ERSPAN monitor source session configuration mode. To remove the configuration, use the `no` form of this command.

```
header-type header-type
no header-type header-type
```

**Syntax Description**

- `header-type` ERSPAN header type. Valid header types are 2 and 3.

**Command Default**

ERSPAN header type is set to 2.

**Command Modes**

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to change the ERSPAN header type to 3:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# header-type 3
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
ip dscp (ERSPAN)

To configure Differentiated Services Code Point (DSCP) values for packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic, use the `ip dscp` command in ERSpan monitor destination session configuration mode. To remove the dscp values, use the `no` form of this command.

```
ip dscp  dscp-value
no ip dscp  dscp-value
```

Syntax Description

- `dscp-value`: DSCP value. Valid values are from 0 to 63.

Command Default

This command has no default behavior or values.

Command Modes

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure DSCP value for ERSpan traffic:

```
Device(config)#  monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)#  ip dscp 15
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Configures an ERSpan destination session and specifies destination properties.</td>
</tr>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSpan source or destination session.</td>
</tr>
</tbody>
</table>
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**

- `ttl-value`: 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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure TTL value for ERSpan traffic:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# ip ttl 32
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Configures an ERSpan destination session and specifies destination properties.</td>
</tr>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSpan source or destination session.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-cache</td>
<td>Specifies the web-cache service (WCCP Version 1 and Version 2).</td>
</tr>
<tr>
<td>service-number</td>
<td>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 <strong>web-cache</strong> keyword.</td>
</tr>
<tr>
<td>group-address groupaddress</td>
<td>(Optional) Specifies the multicast group address used by the device and the application engines to participate in the service group.</td>
</tr>
<tr>
<td>group-list access-list</td>
<td>(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.</td>
</tr>
<tr>
<td>redirect-list access-list</td>
<td>(Optional) Specifies the redirect service for specific hosts or specific packets from hosts.</td>
</tr>
<tr>
<td>password encryption-number password</td>
<td>(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.</td>
</tr>
</tbody>
</table>

### Command Default

WCCP services are not enabled on the device.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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)# 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
```
map platform-type

To set the parameter map attribute filter criteria to platform type, use the `map platform-type` command in parameter-map filter mode. To remove this criteria, use the `no` form of this command.

```
map-number map platform-type {eq | not-eq | regex} platform-type
no map-number map platform-type {eq | not-eq | regex} platform-type
```

<table>
<thead>
<tr>
<th><code>map-number</code></th>
<th>Specifies the parameter map number.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>eq</code></td>
<td>Specifies the filter type name is equal to the platform type name.</td>
</tr>
<tr>
<td><code>not-eq</code></td>
<td>Specifies the filter type name is not equal to the platform type name.</td>
</tr>
<tr>
<td><code>regex</code></td>
<td>Specifies the filter type name is a regular expression.</td>
</tr>
<tr>
<td><code>platform-type</code></td>
<td>Specifies the platform type for the parameter map attribute filter criteria.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled by default.

**Command Modes**

Parameter map filter mode (config-parameter-map-filter)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the parameter map attribute filter criteria to platform type:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type subscriber attribute-to-service Aironet-Policy-para
Device(config-parameter-map-filter)# 10 map platform-type eq C9xxx
```
match platform-type

To evaluate control classes based on the platform type, use the match platform-type command in control class-map filter mode. To remove this condition, use the no form of this command.

```
match platform-type platform-name
no match platform-type platform-name
```

**Syntax Description**
- `platform-name` Specifies the name of the platform.

**Command Default**
This command is disabled by default.

**Command Modes**
Control class-map filter mode (config-filter-control-classmap)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the class map filter to match platform type:

```
Device> enable
Device# configure terminal
Device(config)# class-map type control subscriber match-all DOT1X_NO_AGENT
Device(config-filter-control-classmap)# match platform-type C9xxx
```
**monitor capture (interface/control plane)**

To configure monitor capture points specifying an attachment point and the packet flow direction or add more attachment points to a capture point, use the `monitor capture` command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction or disable one of multiple attachment points on a capture point, use the `no` form of this command.

```
monitor capture {capture-name} {interface interface-type interface-id | control-plane} {in | out | both}
no monitor capture {capture-name} {interface interface-type interface-id | control-plane} {in | out | both}
```

**Syntax Description**

- `capture-name`: The name of the capture to be defined.
- `interface interface-type interface-id`: Specifies an interface with `interface-type` and `interface-id` as an attachment point. The arguments have these meanings:
  - **GigabitEthernet interface-id**: A Gigabit Ethernet IEEE 802.3z interface.
  - **vlan vlan-id**: A VLAN. The range for `vlan-id` is 1 to 4095.
- `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

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:

```plaintext
Device# monitor capture mycap interface GigabitEthernet1/0/1 in
Device# monitor capture mycap match ipv4 any any
```

The second command defines the core filter for the capture point. This is required for a functioning capture point.

To define a capture point with multiple attachment points:

```plaintext
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:

```plaintext
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
```
monitor capture buffer

To configure the buffer for monitor capture (WireShark), use the `monitor capture buffer` command in privileged EXEC mode. To disable the monitor capture buffer or change the buffer back to a default linear buffer from a circular buffer, use the `no` form of this command.

```
monitor capture {capture-name} buffer {circular [size buffer-size] | size buffer-size}
no monitor capture {capture-name} buffer [circular]
```

**Syntax Description**
- `capture-name` The name of the capture whose buffer is to be configured.
- `circular` Specifies that the buffer is of a circular type. The circular type of buffer continues to capture data, even after the buffer is consumed, by overwriting the data captured previously.
- `size buffer-size` (Optional) Specifies the size of the buffer. The range is from 1 MB to 100 MB.

**Command Default**
A linear buffer is configured.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `monitor capture clear` command either during capture or after the capture has stopped either because one or more end conditions have 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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>capture-name</code></td>
<td>The name of the capture to be exported.</td>
</tr>
</tbody>
</table>
| `file-location`    | (Optional) Specifies the location and file name of the capture storage file. Acceptable values for `file-location`:
|                    | • flash—On-board flash storage
|                    | • — USB drive |

**Command Default**
The captured packets are not stored.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:
**monitor capture file**

To configure monitor capture (WireShark) storage file attributes, use the **monitor capture file** command in privileged EXEC mode. To remove a storage file attribute, use the **no** form of this command.

```
monitor capture {capture-name} file { [ buffer-size temp-buffer-size ] [ location file-location : file-name ] [ ring number-of-ring-files ] [ size total-size ] }
no monitor capture {capture-name} file { [ buffer-size ] [ location ] [ ring ] [ size ] }
```

### Syntax Description

- **capture-name**
  The name of the capture to be modified.

- **buffer-size temp-buffer-size**
  (Optional) Specifies the size of the temporary buffer. The range for `temp-buffer-size` is 1 to 100 MB. This is specified to reduce packet loss.

- **location file-location : file-name**
  (Optional) Specifies the location and file name of the capture storage file. Acceptable values for `file-location`:
  - `flash`—On-board flash storage
  - `usb`—USB drive

- **ring number-of-ring-files**
  (Optional) Specifies that the capture is to be stored in a circular file chain and the number of files in the file ring.

- **size total-size**
  (Optional) Specifies the total size of the capture files.

### Command Default

None

### Command Modes

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

Attempts to store packet captures on unsupported devices or devices not connected to the active switch will probably result in errors.
Example

To specify that the storage file name is mycap.pcap, stored on a flash drive:

Device# monitor capture mycap file location flash:mycap.pcap
monitor capture limit

To configure capture limits, use the `monitor capture limit` command in privileged EXEC mode. To remove the capture limits, use the `no` form of this command.

```
monitor capture {capture-name} limit [ {duration seconds} ] [ packet-length size] [ packets num] }
no monitor capture {capture-name} limit [ duration] [ packet-length] [ packets]
```

**Syntax Description**

- `capture-name` (Optional) The name of the capture to be assigned capture limits.
- `duration seconds` (Optional) Specifies the duration of the capture, in seconds. The range is from 1 to 1000000.
- `packet-length size` (Optional) Specifies the packet length, in bytes. If the actual packet is longer than the specified length, only the first set of bytes whose number is denoted by the bytes argument is stored.
- `packets num` (Optional) Specifies the number of packets to be processed for capture.

**Command Default**

Capture limits are not configured.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capture-name</td>
<td>The name of the capture to be assigned a core filter.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies all packets.</td>
</tr>
<tr>
<td>mac mac-match-string</td>
<td>Specifies a Layer 2 packet.</td>
</tr>
<tr>
<td>ipv4</td>
<td>Specifies IPv4 packets.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the host.</td>
</tr>
<tr>
<td>protocol</td>
<td>Specifies the protocol.</td>
</tr>
<tr>
<td>ipv6</td>
<td>Specifies IPv6 packets.</td>
</tr>
</tbody>
</table>

**Command Default**

A core filter is not configured.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `monitor capture clear` command to enable the packet data capture after the capture point is defined. To stop the capture of packet data, use the `monitor capture stop` command.

Ensure that system resources such as CPU and memory are available before starting a capture.

**Example**

To start capturing buffer contents:

```
Device#  monitor capture mycap start
```
monitor capture stop

To stop the capture of packet data at a traffic trace point, use the `monitor capture stop` command in privileged EXEC mode.

```
monitor capture {capture-name} stop
```

**Syntax Description**

- `capture-name` The name of the capture to be stopped.

**Command Default**

The packet data capture is ongoing.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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) or Encapsulated Remote Switched Port Analyzer (ERSPAN) session configuration for analyzing traffic between ports or add to an existing session configuration, use the `monitor session` global configuration command. To clear sessions, use the `no` form of this command.

```
monitor session  session-number  { destination | filter | source | type { erspan-destination | erspan-source } }
no monitor session  { session-number  { destination | filter | source | type { erspan-destination | erspan-source } ] | all | local | range session-range | remote }
```

**Syntax Description**

- `session-number` The session number identified with the session. The range is 1 to 66.
- `all` Clears all monitor sessions.
- `local` Clears all local monitor sessions.
- `range session-range` Clears monitor sessions in the specified range.
- `remote` Clears all remote monitor sessions.

**Command Default**

No monitor sessions are configured.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The `type { erspan-destination</td>
</tr>
<tr>
<td></td>
<td>This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>The `type { erspan-destination</td>
</tr>
<tr>
<td></td>
<td>This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

**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, RSPAN, and ERSPAN 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, FRSPAN, and ERSPAN 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**

<table>
<thead>
<tr>
<th><strong>session-number</strong></th>
<th>The session number identified with the SPAN or RSPAN session. The range is 1 to 66.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>interface interface-id</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>,</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>-</strong></td>
<td>(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.</td>
</tr>
<tr>
<td><strong>encapsulation replicate</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>encapsulation dot1q</strong></td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**
Enables ingress traffic forwarding.

**dot1q**
(Optional) Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.

**untagged**
(Optional) Accepts incoming packets with untagged encapsulation with the specified VLAN as the default VLAN.

**isl**
Specifies ingress forwarding using ISL encapsulation.

**remote**
Specifies the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.

The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).

**vlan vlan-id**
Sets the default VLAN for ingress traffic when used with only the `ingress` keyword.

---

**Command Default**
No monitor sessions are configured.

If `encapsulation replicate` is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

You can specify `all`, `local`, `range session-range`, or `remote` with the `no monitor session` command to clear all SPAN and RSPAN, all local SPAN, a range, or all RSPAN sessions.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session-number</code></td>
<td>The session number identified with the SPAN or RSPAN session. The range is 1 to 66.</td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td>Specifies a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The <code>vlan-id</code> range is 1 to 4094.</td>
</tr>
<tr>
<td><code>,</code></td>
<td>(Optional) Specifies a series of VLANs, or separates a range of VLANs from a previous range. Enter a space before and after the comma.</td>
</tr>
<tr>
<td><code>-</code></td>
<td>(Optional) Specifies a range of VLANs. Enter a space before and after the hyphen.</td>
</tr>
</tbody>
</table>

### Command Default

No monitor sessions are configured.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 `,` or `-` 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:

Device(config)# monitor session 1 source interface gigabitethernet1/0/1 both
Device(config)# monitor session 1 destination interface gigabitethernet1/0/2
Device(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.

```bash
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>session_number</code></td>
<td>The session number identified with the SPAN or RSPAN session. The range is 1 to 66.</td>
</tr>
<tr>
<td><code>interface interface-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>,</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>-</code></td>
<td>(Optional) Specifies a range of interfaces or VLANs. Enter a space before and after the hyphen.</td>
</tr>
<tr>
<td>`both</td>
<td>rx</td>
</tr>
<tr>
<td><code>remote</code></td>
<td>(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).</td>
</tr>
<tr>
<td><code>vlan vlan-id</code></td>
<td>When used with only the <code>ingress</code> keyword, sets default VLAN for ingress traffic.</td>
</tr>
</tbody>
</table>

### 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
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

To configure a local Encapsulated Remote Switched Port Analyzer (ERSPAN) session, use the `monitor session type` command in global configuration mode. To remove the ERSPAN configuration, use the `no` form of this command.

```
monitor session span-session-number type {erspan-destination | erspan-source}  
no monitor session span-session-number type {erspan-destination | erspan-source}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>span-session-number</code></td>
<td>Number of the local ERSPAN session. Valid values are from 1 to 66.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERSPAN source or destination session is not configured.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration (config)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
<td><strong>Modification</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
| Cisco IOS XE Fuji 16.9.1 | The `erspan-destination` keyword was introduced.  
This was implemented on the Cisco Catalyst 9500 Series High Performance Switches. |
| Cisco IOS XE Gibraltar 16.11.1 | The `erspan-destination` keyword was introduced.  
This was implemented on the Cisco Catalyst 9500 Series Switches. |

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The <code>span-session-number</code> and the session type cannot be changed once configured. Use the <code>no</code> form of this command to remove the session and then re-create the session with a new session ID or a new session type.</td>
<td></td>
</tr>
<tr>
<td>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 <code>ip address</code> command in ERSPAN monitor destination session configuration mode.</td>
<td></td>
</tr>
<tr>
<td>The ERSPAN ID differentiates the ERSPAN traffic arriving at the same destination IP address from different ERSPAN source sessions.</td>
<td></td>
</tr>
<tr>
<td>The maximum local ERSPAN source session limit is 8.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following example shows how to configure an ERSPAN source session number:</td>
<td></td>
</tr>
</tbody>
</table>

```
Device(config)# monitor session 55 type erspan-source  
Device(config-mon-erspan-src)#
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>monitor session type</strong></td>
<td>Creates an ERSPAN source or destination session number or enters the ERSPAN session configuration mode for the session.</td>
</tr>
<tr>
<td><strong>show capability feature monitor</strong></td>
<td>Displays information about monitor features.</td>
</tr>
<tr>
<td><strong>show monitor session</strong></td>
<td>Displays information about the ERSPAN, SPAN, and RSPAN sessions.</td>
</tr>
</tbody>
</table>
**mtu (ERSPAN)**

To configure the maximum transmission unit (MTU) size for ERSPAN truncation, use the `mtu` command in ERSPAN monitor destination session configuration mode. To restore the MTU value to its original default value, use the `no` form of this command.

```
mtu  bytes
no  mtu
```

**Syntax Description**

- `bytes` MTU size, in bytes. The default value of MTU is 9000 bytes.

**Command Modes**

ERSPAN monitor destination session configuration mode (config-mon-erspan-src-dst)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced. This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# destination
Device(config-mon-erspan-src-dst)# mtu 1000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Configures an ERSPAN destination session and specifies destination properties.</td>
</tr>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

ERSPAN source session on a switch can use different source IP addresses using the `origin` command.

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
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Configures an ERSPAN destination session and specifies destination properties.</td>
</tr>
<tr>
<td>monitor session type erspan-source</td>
<td>Configures a local ERSPAN source session.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>erspan-destination</td>
<td>Displays information about the configured Encapsulated Remote Switched Port Analyzer (ERSPAN) source sessions.</td>
</tr>
<tr>
<td>erspan-source</td>
<td>Displays all the configured global built-in templates.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 ERSSPAN source session: 8
No of Tx ERSSPAN source session: 8
ERSPAN Header Type supported: II
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session type erspan-source</td>
<td>Creates an ERSSPAN source session number or enters the ERSSPAN session configuration mode for the session.</td>
</tr>
</tbody>
</table>
show class-map type control subscriber

To display class map statistics for the configured control policies, use the `show class-map type control subscriber` command in privileged EXEC mode.

```
show class-map type control subscriber {all | name control-class-name}
```

### Syntax Description

- **all**
  - Displays class map statistics for all control policies.

- **name control-class-name**
  - Displays class map statistics for the specified control policy.

### Command Modes

- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following is a sample output of the `show class-map type control subscriber name control-class-name` command:

```
Device# show class-map type control subscriber name platform

<table>
<thead>
<tr>
<th>Class-map</th>
<th>Action</th>
<th>Exec</th>
<th>Hit</th>
<th>Miss</th>
<th>Comp</th>
</tr>
</thead>
<tbody>
<tr>
<td>match-all</td>
<td>platform</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Key:
- "Exec" - The number of times this line was executed
- "Hit" - The number of times this line evaluated to TRUE
- "Miss" - The number of times this line evaluated to FALSE
- "Comp" - The number of times this line completed the execution of its condition without a need to continue on to the end
```
show ip sla statistics

To display current or aggregated operational status and statistics of all Cisco IOS IP Service Level Agreement (SLA) operations or a specified operation, use the `show ip sla statistics` command in user EXEC or privileged EXEC mode.

```
show ip sla statistics [ operation-number [ details ] ] | aggregated [ operation-number | details ]
```

**Syntax Description**

- `operation-number` (Optional) Number of the operation for which operational status and statistics are displayed. Accepted values are from 1 to 2147483647.
- `details` (Optional) Specifies detailed output.
- `aggregated` (Optional) Specifies the IP SLA aggregated statistics.

**Command Default**

Displays output for all running IP SLA operations.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 Oper Sense: ok
Latest Sense Description: 200 OK
```
Total RTT: 544
DNS RTT: 12
TCP Connection RTT: 28
HTTP Transaction RTT: 504
HTTP Message Size: 9707
show monitor

To display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions, use the `show monitor` command in EXEC mode.

```
show monitor [session {session_number | all | local | range list | remote} [detail]]
```

**Syntax Description**

- **session**
  - (Optional) Displays information about specified SPAN sessions.

- **session_number**
  - The session number identified with the SPAN or RSPAN session. The range is 1 to 66.

- **all**
  - (Optional) Displays all SPAN sessions.

- **local**
  - (Optional) Displays only local SPAN sessions.

- **range list**
  - (Optional) Displays a range of SPAN sessions, where `list` is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.

  **Note**
  - This keyword is available only in privileged EXEC mode.

- **remote**
  - (Optional) Displays only remote SPAN sessions.

- **detail**
  - (Optional) Displays detailed information about the specified sessions.

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

- **Release**
  - Cisco IOS XE Everest 16.5.1a

  **Modification**
  - 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**

- `capture-name` *(Optional)* Specifies the name of the capture to be displayed.
- `buffer` *(Optional)* Specifies that a buffer associated with the named capture is to be displayed.
- `file file-location : file-name` *(Optional)* Specifies the file location and name of the capture storage file to be displayed.
- `brief` *(Optional)* Specifies the display content in brief.
- `detailed` *(Optional)* Specifies detailed display content.
- `display-filter display-filter-string` Filters the display content according to the `display-filter-string`.

**Command Default**

Displays all capture content.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 Switched Port Analyzer (SPAN), Remote SPAN (RSPAN), and Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions, use the `show monitor session` command in EXEC mode.

```
show monitor session {session_number | all | erspan-destination | erspan-source | local | range list | remote} [detail]
```

**Syntax Description**

- `session_number` - The session number identified with the SPAN or RSPAN session. The range is 1 to 66.
- `all` - Displays all SPAN sessions.
- `erspan-source` - Displays only source ERSPAN sessions.
- `erspan-destination` - Displays only destination ERSPAN sessions.
- `local` - Displays only local SPAN sessions.
- `range list` - Displays a range of SPAN sessions, where `list` is the range of valid sessions. The range is either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.

**Note** This keyword is available only in privileged EXEC mode.

- `remote` - Displays only remote SPAN sessions.
- `detail` - (Optional) Displays detailed information about the specified sessions.

**Command Modes**

- User EXEC (>

- Privileged EXEC(#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>The <code>erspan-destination</code> keyword was introduced. This was implemented on the Cisco Catalyst 9500 Series High Performance Switches.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>The <code>erspan-destination</code> keyword was introduced. This was implemented on the Cisco Catalyst 9500 Series Switches.</td>
</tr>
</tbody>
</table>
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:

```
Device# 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
```

The following is sample output from the `show monitor session erspan-destination` command:

```
Device# show monitor session erspan-destination
Type : ERSPAN Destination Session
```
show monitor session

<table>
<thead>
<tr>
<th>Status</th>
<th>Admin Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP Address</td>
<td>10.10.10.210</td>
</tr>
<tr>
<td>Source ERSPAN ID</td>
<td>40</td>
</tr>
</tbody>
</table>
show parameter-map type subscriber attribute-to-service

To display parameter map statistics, use the `show parameter-map type subscriber attribute-to-service` command in privileged EXEC mode.

`show parameter-map type subscriber attribute-to-service {all | name parameter-map-name}`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Displays statistics for all parameter maps.</td>
</tr>
<tr>
<td><code>name parameter-map-name</code></td>
<td>Displays statistics for the specified parameter map.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (`#`)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample output of the `show parameter-map type subscriber attribute-to-service name parameter-map-name` command:

```
Device# show parameter-map type subscriber attribute-to-service name platform

Parameter-map name: platform
Map: 10 platform-type regex "C9xxx"
Action(s):
   10 interface-template critical
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 14_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 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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch</td>
<td>Displays information about the switch.</td>
</tr>
<tr>
<td>F0</td>
<td>Displays information about the Embedded Service Processor (ESP) slot 0.</td>
</tr>
<tr>
<td>FP</td>
<td>Displays information about the ESP.</td>
</tr>
<tr>
<td>active</td>
<td>Displays information about the active instance of the ESP or the Route Processor (RP).</td>
</tr>
<tr>
<td>counters</td>
<td>Displays the SWSPAN message counters.</td>
</tr>
<tr>
<td>R0</td>
<td>Displays information about the RP slot 0.</td>
</tr>
<tr>
<td>RP</td>
<td>Displays information about the RP.</td>
</tr>
<tr>
<td>destination sess-id session-ID</td>
<td>Displays information about the specified destination session.</td>
</tr>
<tr>
<td>source sess-id session-ID</td>
<td>Displays information about the specified source session.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

Release | Modification
---------|---------------------
Cisco IOS XE Everest 16.5.1a | 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
Inf Type : PORT
Port dpidx : 30
FD Sess ID : 1
Session Type : Local
Direction : Ingress
Filter Enabled : No
ACL Configured : No
AOM Object id : 579
AOM Object Status : Done
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
snmp ifmib ifindex persist

To globally enable ifIndex values to persist, which will remain constant across reboots, for use by the Simple Network Management Protocol (SNMP), use the `snmp ifmib ifindex persist` command in global configuration mode. To globally disable ifIndex persistence, use the `no` form of this command.

`snmp ifmib ifindex persist`
`no snmp ifmib ifindex persist`

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

**Command Default**
The ifIndex persistence on a device is disabled.

**Command Modes**
Global configuration (config)

**Usage Guidelines**
The `snmp ifmib ifindex persist` command does not override an interface-specific configuration. The interface-specific configuration of ifIndex persistence is configured with the `snmp ifindex persist` and `snmp ifindex clear` commands in interface configuration mode.

The `snmp ifmib ifindex persist` command enables ifIndex persistence for all interfaces on a routing device by using the ifDescr and ifIndex entries in the ifIndex table of interface MIB (IF-MIB).

IfIndex persistence means that the ifIndex values in the IF-MIB persist across reboots, allowing for the consistent identification of specific interfaces that use SNMP.

If ifIndex persistence was previously disabled for a specific interface by using the `no snmp ifindex persist` command, ifIndex persistence will remain disabled for that interface.

**Examples**
The following example shows how to enable ifIndex persistence for all interfaces:

```
Device(config)# snmp ifmib ifindex persist
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp ifindex clear</td>
<td>Clears any previously configured <code>snmp ifindex</code> commands issued in interface configuration mode for a specific interface.</td>
</tr>
<tr>
<td>snmp ifindex persist</td>
<td>Enables ifIndex values that persist across reboots (ifIndex persistence) in the IF-MIB.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-framework</td>
<td>(Optional) Enables SNMP CISCO-AUTH-FRAMEWORK-MIB traps.</td>
</tr>
<tr>
<td>sec-violation</td>
<td>(Optional) Enables SNMP camSecurityViolationNotif notifications.</td>
</tr>
<tr>
<td>bridge</td>
<td>(Optional) Enables SNMP STP Bridge MIB traps.</td>
</tr>
<tr>
<td>call-home</td>
<td>(Optional) Enables SNMP CISCO-CALLHOME-MIB traps.</td>
</tr>
<tr>
<td>cluster</td>
<td>(Optional) Enables SNMP cluster traps.</td>
</tr>
<tr>
<td>config</td>
<td>(Optional) Enables SNMP configuration traps.</td>
</tr>
<tr>
<td>config-copy</td>
<td>(Optional) Enables SNMP configuration copy traps.</td>
</tr>
<tr>
<td>config-ctid</td>
<td>(Optional) Enables SNMP configuration CTID traps.</td>
</tr>
<tr>
<td>copy-config</td>
<td>(Optional) Enables SNMP copy-configuration traps.</td>
</tr>
<tr>
<td>cpu</td>
<td>(Optional) Enables CPU notification traps.</td>
</tr>
<tr>
<td>dot1x</td>
<td>(Optional) Enables SNMP dot1x traps.</td>
</tr>
<tr>
<td>energywise</td>
<td>(Optional) Enables SNMP energywise traps.</td>
</tr>
<tr>
<td>entity</td>
<td>(Optional) Enables SNMP entity traps.</td>
</tr>
<tr>
<td>envmon</td>
<td>(Optional) Enables SNMP environmental monitor traps.</td>
</tr>
<tr>
<td>errdisable</td>
<td>(Optional) Enables SNMP errdisable notification traps.</td>
</tr>
<tr>
<td>event-manager</td>
<td>(Optional) Enables SNMP Embedded Event Manager traps.</td>
</tr>
<tr>
<td>flash</td>
<td>(Optional) Enables SNMP FLASH notification traps.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fru-ctrl</td>
<td>(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.</td>
</tr>
<tr>
<td>license</td>
<td>(Optional) Enables license traps.*</td>
</tr>
<tr>
<td>mac-notification</td>
<td>(Optional) Enables SNMP MAC Notification traps.*</td>
</tr>
<tr>
<td>port-security</td>
<td>(Optional) Enables SNMP port security traps.*</td>
</tr>
<tr>
<td>power-ethernet</td>
<td>(Optional) Enables SNMP power Ethernet traps.*</td>
</tr>
<tr>
<td>rep</td>
<td>(Optional) Enables SNMP Resilient Ethernet Protocol traps.</td>
</tr>
<tr>
<td>snmp</td>
<td>(Optional) Enables SNMP traps.*</td>
</tr>
<tr>
<td>stackwise</td>
<td>(Optional) Enables SNMP stackwise traps.*</td>
</tr>
<tr>
<td>storm-control</td>
<td>(Optional) Enables SNMP storm-control trap parameters.*</td>
</tr>
<tr>
<td>stpx</td>
<td>(Optional) Enables SNMP STPX MIB traps.*</td>
</tr>
<tr>
<td>syslog</td>
<td>(Optional) Enables SNMP syslog traps.</td>
</tr>
<tr>
<td>transceiver</td>
<td>(Optional) Enables SNMP transceiver traps.*</td>
</tr>
<tr>
<td>tty</td>
<td>(Optional) Sends TCP connection traps. This is enabled by default.</td>
</tr>
<tr>
<td>vlan-membership</td>
<td>(Optional) Enables SNMP VLAN membership traps.</td>
</tr>
<tr>
<td>vlancreate</td>
<td>(Optional) Enables SNMP VLAN-created traps.</td>
</tr>
<tr>
<td>vlandelete</td>
<td>(Optional) Enables SNMP VLAN-deleted traps.</td>
</tr>
<tr>
<td>vstack</td>
<td>(Optional) Enables SNMP Smart Install traps.*</td>
</tr>
<tr>
<td>vtp</td>
<td>(Optional) Enables VLAN Trunking Protocol (VTP) traps.</td>
</tr>
</tbody>
</table>

**Command Default**
The sending of SNMP traps is disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
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:

```bash
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**
- `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Specify the host (NMS) that receives the traps by using the `snmp-server host` global configuration command. If no trap types are specified, all trap types are sent.

**Note**
Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate `snmp-server enable traps` command for each trap type.

**Examples**

This example shows how to generate SNMP CEF inconsistency traps:

```
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.

```bash
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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```bash
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify the host (NMS) that receives the traps by using the `snmp-server host` global configuration command. If no trap types are specified, all trap types are sent.

**Note**
Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate `snmp-server enable traps` command for each trap type.

**Examples**

This example shows how to generate fan traps:

```
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.

```
no snmp-server enable traps errdisable
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>notification-rate number-of-notifications</code></td>
<td>(Optional) Specifies number of notifications per minute as the notification rate. Accepted values are from 0 to 10000.</td>
</tr>
</tbody>
</table>

### Command Default

The sending of SNMP notifications of error-disabling is disabled.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify the host (NMS) that receives the traps by using the `snmp-server host` global configuration command. If no trap types are specified, all trap types are sent.

**Note**

Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate `snmp-server enable traps` command for each trap type.

**Examples**

This example shows how to generate license deployment traps:

```
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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>change</td>
<td>(Optional) Enables SNMP MAC change traps.</td>
</tr>
<tr>
<td>move</td>
<td>(Optional) Enables SNMP MAC move traps.</td>
</tr>
<tr>
<td>threshold</td>
<td>(Optional) Enables SNMP MAC threshold traps.</td>
</tr>
</tbody>
</table>

**Command Default**
The sending of SNMP MAC notification traps is disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-specific</td>
<td>(Optional) Enables Cisco-specific traps.</td>
</tr>
<tr>
<td>errors</td>
<td>(Optional) Enables error traps.</td>
</tr>
<tr>
<td>lsa</td>
<td>(Optional) Enables link-state advertisement (LSA) traps.</td>
</tr>
<tr>
<td>rate-limit</td>
<td>(Optional) Enables rate-limit traps.</td>
</tr>
<tr>
<td>rate-limit-time</td>
<td>(Optional) Specifies window of time in seconds for rate-limit traps. Accepted values are 2 to 60.</td>
</tr>
<tr>
<td>max-number-of-traps</td>
<td>(Optional) Specifies maximum number of rate-limit traps to be sent in window time.</td>
</tr>
<tr>
<td>retransmit</td>
<td>(Optional) Enables packet-retransmit traps.</td>
</tr>
<tr>
<td>state-change</td>
<td>(Optional) Enables state-change traps.</td>
</tr>
</tbody>
</table>

**Command Default**

The sending of OSPF SNMP traps is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```
sh 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
% no snmp-server enable traps port-security
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>trap-rate value</code></td>
<td>(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).</td>
</tr>
</tbody>
</table>

**Command Default**
The sending of port security SNMP traps is disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group number</code></td>
<td>Enables inline power group-based traps for the specified group number. Accepted values are from 1 to 9.</td>
</tr>
<tr>
<td><code>police</code></td>
<td>Enables inline power policing traps.</td>
</tr>
</tbody>
</table>

**Command Default**
The sending of power-over-Ethernet SNMP traps is disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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-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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Specify the host (NMS) that receives the traps by using the `snmp-server host` global configuration command. If no trap types are specified, all trap types are sent.

**Note**
Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate `snmp-server enable traps` command for each trap type.

**Examples**

This example shows how to enable a warmstart SNMP trap:

```
Device(config)# snmp-server enable traps snmp warmstart
```
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.

```
no snmp-server enable traps storm-control {trap-rate number-of-minutes}
```

Syntax Description

- **trap-rate**
  - (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 STP X 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 STP X MIB inconsistency update traps.
- `loop-inconsistency` (Optional) Enables SNMP STP X MIB loop inconsistency update traps.
- `root-inconsistency` (Optional) Enables SNMP STP X MIB root inconsistency update traps.

**Command Default**

The sending of SNMP STP X MIB traps is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 STP X MIB inconsistency update traps:

```
Device(config)# snmp-server enable traps stpx inconsistency
```
snmp-server enable traps transceiver

To enable SNMP transceiver traps, use the `snmp-server enable traps transceiver` command in global configuration mode. Use the `no` form of this command to return to the default setting.

```
snmp-server enable traps transceiver {all}
no snmp-server enable traps transceiver {all}
```

**Syntax Description**

- `all` (Optional) Enables all SNMP transceiver traps.

**Command Default**

The sending of SNMP transceiver traps is disabled.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vnet-trunk-down</td>
<td>(Optional) Enables vrfmib trunk down traps.</td>
</tr>
<tr>
<td>vnet-trunk-up</td>
<td>(Optional) Enables vrfmib trunk up traps.</td>
</tr>
<tr>
<td>vrf-down</td>
<td>(Optional) Enables vrfmib vrf down traps.</td>
</tr>
<tr>
<td>vrf-up</td>
<td>(Optional) Enables vrfmib vrf up traps.</td>
</tr>
</tbody>
</table>

**Command Default**
The sending of SNMP vrfmib traps is disabled.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 separate `snmp-server enable traps` commands 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

- **local engineid-string** Specifies a 24-character ID string with the name of the copy of SNMP. You need not specify the entire 24-character engine ID if it has trailing zeros. Specify only the portion of the engine ID up to the point where only zeros remain in the value.

- **remote ip-address** Specifies the remote SNMP copy. Specify the `ip-address` of the device that contains the remote copy of SNMP.

- **udp-port port-number** (Optional) Specifies the User Datagram Protocol (UDP) port on the remote device. The default is 162.

### Command Default

An SNMP engine ID is generated automatically but is not displayed or stored in the running configuration. You can display the default or configured engine ID by using the `show snmp engineID` command.

In a common scenario, once the customer sets up SNMP, they use this auto-generated engineID. However, when a switch is running on StackWise Virtual, it is based on the active switch mac address.

If a stack reloads, and another switch of the stack boots first and is elected as standby, then the SNMPv3 engineID will be different. This causes failures in the SNMP environment and can be avoided by defining the `snmp-server engineID local engineid-string`.

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

None

### Examples

The following example configures a local engine ID of 123400000000000000000000:

```
Device(config)# snmp-server engineID local 1234
```
snmp-server group

To configure a new Simple Network Management Protocol (SNMP) group, use the `snmp-server group` command in global configuration mode. To remove a specified SNMP group, use the `no` form of this command.

```
snmp-server group group-name {v1 | v2c | v3 {auth | noauth | priv}} {context context-name} [match {exact | prefix}] [read read-view] [write write-view] [notify notify-view] [access [ipv6 named-access-list] [{acl-number acl-name}]]
```

```
no snmp-server group group-name {v1 | v2c | v3 {auth | noauth | priv}} {context context-name}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group-name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>v1</td>
<td>Specifies that the group is using the SNMPv1 security model. SNMPv1 is the least secure of the possible SNMP security models.</td>
</tr>
<tr>
<td>v2c</td>
<td>Specifies that the group is using the SNMPv2c security model. The SNMPv2c security model allows informs to be transmitted and supports 64-character strings.</td>
</tr>
<tr>
<td>v3</td>
<td>Specifies that the group is using the SNMPv3 security model. SNMPv3 is the most secure of the supported security models. It allows you to explicitly configure authentication characteristics.</td>
</tr>
<tr>
<td>auth</td>
<td>Specifies authentication of a packet without encrypting it.</td>
</tr>
<tr>
<td>noauth</td>
<td>Specifies no authentication of a packet.</td>
</tr>
<tr>
<td>priv</td>
<td>Specifies authentication of a packet with encryption.</td>
</tr>
<tr>
<td>context</td>
<td>(Optional) Specifies the SNMP context to associate with this SNMP group and its views.</td>
</tr>
<tr>
<td>context-name</td>
<td>(Optional) Context name.</td>
</tr>
<tr>
<td>match</td>
<td>(Optional) Specifies an exact context match or matches only the context prefix.</td>
</tr>
<tr>
<td>exact</td>
<td>(Optional) Matches the exact context.</td>
</tr>
<tr>
<td>prefix</td>
<td>(Optional) Matches only the context prefix.</td>
</tr>
<tr>
<td>read</td>
<td>(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.</td>
</tr>
<tr>
<td>read-view</td>
<td>(Optional) String of a maximum of 64 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the read option is used to override this state.</td>
</tr>
<tr>
<td>write</td>
<td>(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.</td>
</tr>
</tbody>
</table>
**write-view** *(Optional) String of a maximum of 64 characters that is the name of the view.*

The default is that nothing is defined for the write view (that is, the null OID). You must configure write access.

**notify** *(Optional) Specifies a notify view for the SNMP group. This view enables you to specify a notify, inform, or trap.*

**notify-view** *(Optional) String of a maximum of 64 characters that is the name of the view.*

By default, nothing is defined for the notify view (that is, the null OID) until the **snmp-server host** command is configured. If a view is specified in the **snmp-server group** command, any notifications in that view that are generated will be sent to all users associated with the group (provided a SNMP server host configuration exists for the user).

Cisco recommends that you let the software autogenerate the notify view. See the “Configuring Notify Views” section in this document.

**access** *(Optional) Specifies a standard access control list (ACL) to associate with the group.*

**ipv6** *(Optional) Specifies an IPv6 named access list. If both IPv6 and IPv4 access lists are indicated, the IPv6 named access list must appear first in the list.*

**named-access-list** *(Optional) Name of the IPv6 access list.*

**acl-number** *(Optional) The acl-number argument is an integer from 1 to 99 that identifies a previously configured standard access list.*

**acl-name** *(Optional) The acl-name argument is a string of a maximum of 64 characters that is the name of a previously configured standard access list.*

---

**Command Default**

No SNMP server groups are configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When a community string is configured internally, two groups with the name public are autogenerated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name public and a v2c group with the name public.

No default values exist for authentication or privacy algorithms when you configure the **snmp-server group** command. Also, no default passwords exist. For information about specifying a Message Digest 5 (MD5) password, see the documentation of the **snmp-server user** command.

**Configuring Notify Views**

The notify-view option is available for two reasons:

- If a group has a notify view that is set using SNMP, you may need to change the notify view.
• The `snmp-server host` command may have been configured before the `snmp-server group` command. In this case, you must either reconfigure the `snmp-server host` command, or specify the appropriate notify view.

Specifying a notify view when configuring an SNMP group is not recommended, for the following reasons:

• The `snmp-server host` command autogenerates a notify view for the user, and then adds it to the group associated with that user.

• Modifying the group’s notify view will affect all users associated with that group.

Instead of specifying the notify view for a group as part of the `snmp-server group` command, use the following commands in the order specified:

1. `snmp-server user`—Configures an SNMP user.
2. `snmp-server group`—Configures an SNMP group, without adding a notify view.
3. `snmp-server host`—Autogenerates the notify view by specifying the recipient of a trap operation.

**SNMP Contexts**

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN’s specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

Use this command with the `context context-name` keyword and argument to associate a read, write, or notify SNMP view with an SNMP context.

**Create an SNMP Group**

The following example shows how to create the SNMP server group “public,” allowing read-only access for all objects to members of the standard named access list “lmnop”:

```
Device(config)# snmp-server group public v2c access lmnop
```

**Remove an SNMP Server Group**

The following example shows how to remove the SNMP server group “public” from the configuration:

```
Device(config)# no snmp-server group public v2c
```

**Associate an SNMP Server Group with Specified Views**

The following example shows SNMP context “A” associated with the views in SNMPv2c group “GROUP1”:

```
Device(config)# snmp-server context A
Device(config)# snmp mib community commA
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show snmp group</td>
<td>Displays the names of groups on the device and the security model, the status</td>
</tr>
<tr>
<td></td>
<td>of the different views, and the storage type of each group.</td>
</tr>
<tr>
<td>snmp mib community-map</td>
<td>Associates a SNMP community with an SNMP context, engine ID, security</td>
</tr>
<tr>
<td></td>
<td>name, or VPN target list.</td>
</tr>
<tr>
<td>snmp-server host</td>
<td>Specifies the recipient of a SNMP notification operation.</td>
</tr>
<tr>
<td>snmp-server user</td>
<td>Configures a new user to a SNMP group.</td>
</tr>
</tbody>
</table>
To specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation, use the `snmp-server host` global configuration command on the device. Use the `no` form of this command to remove the specified host.

```
snmp-server host { host-addr } [ vrf vrf-instance ] [ informs | traps ] [ version { 1 | 2c | 3 } { auth | noauth | priv } ] { community-string [ notification-type ] }
no snmp-server host { host-addr } [ vrf vrf-instance ] [ informs | traps ] [ version { 1 | 2c | 3 } { auth | noauth | priv } ] { community-string [ notification-type ] }
```

**Syntax Description**
- `host-addr` (Name or Internet address of the host (the targeted recipient)).
- `vrf vrf-instance` (Optional) Specifies the virtual private network (VPN) routing instance and name for this host.
- `informs | traps` (Optional) Sends SNMP traps or informs to this host.
- `version { 1 | 2c | 3 }` (Optional) Specifies the version of the SNMP used to send the traps.
  - `1`—SNMPv1. This option is not available with informs.
  - `2c`—SNMPv2C.
  - `3`—SNMPv3. One of the authorization keywords (see next table row) must follow the Version 3 keyword.
- `auth | noauth | priv` (Optional) Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.
  - `noauth` (Default)—The noAuthNoPriv security level. This is the default if the `auth | noauth | priv` keyword choice is not specified.
  - `priv` (Optional)—Enables Data Encryption Standard (DES) packet encryption (also called privacy).
- `community-string` (Password-like community string sent with the notification operation. Though you can set this string by using the `snmp-server host` command, we recommend that you define this string by using the `snmp-server community` global configuration command before using the `snmp-server host` command.
  - **Note** The `@` symbol is used for delimiting the context information. Avoid using the `@` symbol as part of the SNMP community string when configuring this command.
**notification-type** (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:

- **auth-framework**—Sends SNMP CISCO-AUTH-FRAMEWORK-MIB traps.
- **bridge**—Sends SNMP Spanning Tree Protocol (STP) bridge MIB traps.
- **bulkstat**—Sends Data-Collection-MIB Collection notification traps.
- **call-home**—Sends SNMP CISCO-CALLHOME-MIB traps.
- **cef**—Sends SNMP CEF traps.
- **config**—Sends SNMP configuration traps.
- **config-copy**—Sends SNMP config-copy traps.
- **config-ctid**—Sends SNMP config-ctid traps.
- **copy-config**—Sends SNMP copy configuration traps.
- **cpu**—Sends CPU notification traps.
- **cpu threshold**—Sends CPU threshold notification traps.
- **eigrp**—Sends SNMP EIGRP traps.
- **entity**—Sends SNMP entity traps.
snmp-server host

- **envmon**—Sends environmental monitor traps.
- **errdisable**—Sends SNMP errdisable notification traps.
- **event-manager**—Sends SNMP Embedded Event Manager traps.
- **flash**—Sends SNMP FLASH notifications.
- **flowmon**—Sends SNMP flowmon notification traps.
- **ipmulticast**—Sends SNMP IP multicast routing traps.
- **ipsla**—Sends SNMP IP SLA traps.
- **isis**—Sends IS-IS traps.
- **license**—Sends license traps.
- **local-auth**—Sends SNMP local auth traps.
- **mac-notification**—Sends SNMP MAC notification traps.
- **ospf**—Sends Open Shortest Path First (OSPF) traps.
- **pim**—Sends SNMP Protocol-Independent Multicast (PIM) traps.
- **port-security**—Sends SNMP port-security traps.
- **power-ethernet**—Sends SNMP power Ethernet traps.
- **snmp**—Sends SNMP-type traps.
- **storm-control**—Sends SNMP storm-control traps.
- **stpx**—Sends SNMP STP extended MIB traps.
- **syslog**—Sends SNMP syslog traps.
- **transceiver**—Sends SNMP transceiver traps.
- **tty**—Sends TCP connection traps.
- **vlan-membership**—Sends SNMP VLAN membership traps.
- **vланcreate**—Sends SNMP VLAN-created traps.
- **vlandelete**—Sends SNMP VLAN-deleted traps.
- **vrfmib**—Sends SNMP vrfmib traps.
- **vstack**—Sends SNMP Smart Install traps.
- **vtp**—Sends SNMP VLAN Trunking Protocol (VTP) traps.
- **wireless**—Sends wireless traps.

**Command Default**

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.
If no `version` keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the `noauth` (noAuthNoPriv) security level.

---

**Note**

Though visible in the command-line help strings, the `fru-ctrl` keyword is not supported.

---

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```none
snmp-server host example traps v3 <community-string> auth <mode> authKey <key>
```
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.
snmp-server user

To configure a new user to a Simple Network Management Protocol (SNMP) group, use the `snmp-server user` command in global configuration mode. To remove a user from an SNMP group, use the `no` form of this command.

```
snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes {128 | 192 | 256}} privpassword] {acl-number acl-name}]
no snmp-server user username group-name [remote host [udp-port port] [vrf vrf-name]] {v1 | v2c | v3 [encrypted] [auth {md5 | sha} auth-password]} [access [ipv6 nacl] [priv {des | 3des | aes {128 | 192 | 256}} privpassword] {acl-number acl-name}]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>username</code></td>
<td>Name of the user on the host that connects to the agent.</td>
</tr>
<tr>
<td><code>group-name</code></td>
<td>Name of the group to which the user belongs.</td>
</tr>
<tr>
<td><code>remote</code></td>
<td>(Optional) Specifies a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>(Optional) Name or IP address of the remote SNMP host.</td>
</tr>
<tr>
<td><code>udp-port</code></td>
<td>(Optional) Specifies the User Datagram Protocol (UDP) port number of the remote host.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>(Optional) Integer value that identifies the UDP port. The default is 162.</td>
</tr>
<tr>
<td><code>vrf</code></td>
<td>(Optional) Specifies an instance of a routing table.</td>
</tr>
<tr>
<td><code>vrf-name</code></td>
<td>(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.</td>
</tr>
<tr>
<td><code>v1</code></td>
<td>Specifies that SNMPv1 should be used.</td>
</tr>
<tr>
<td><code>v2c</code></td>
<td>Specifies that SNMPv2c should be used.</td>
</tr>
<tr>
<td><code>v3</code></td>
<td>Specifies that the SNMPv3 security model should be used. Allows the use of the <code>encrypted</code> keyword or <code>auth</code> keyword or both.</td>
</tr>
<tr>
<td><code>encrypted</code></td>
<td>(Optional) Specifies whether the password appears in encrypted format.</td>
</tr>
<tr>
<td><code>auth</code></td>
<td>(Optional) Specifies which authentication level should be used.</td>
</tr>
<tr>
<td><code>md5</code></td>
<td>(Optional) Specifies the HMAC-MD5-96 authentication level.</td>
</tr>
<tr>
<td><code>sha</code></td>
<td>(Optional) Specifies the HMAC-SHA-96 authentication level.</td>
</tr>
<tr>
<td><code>auth-password</code></td>
<td>(Optional) String (not to exceed 64 characters) that enables the agent to receive packets from the host.</td>
</tr>
<tr>
<td><code>access</code></td>
<td>(Optional) Specifies an Access Control List (ACL) to be associated with this SNMP user.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Specifies an IPv6 named access list to be associated with this SNMP user.</td>
</tr>
<tr>
<td>Argument</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>nacl</td>
<td>(Optional) Name of the ACL. IPv4, IPv6, or both IPv4 and IPv6 access lists may be specified. If both are specified, the IPv6 named access list must appear first in the statement.</td>
</tr>
<tr>
<td>priv</td>
<td>(Optional) Specifies the use of the User-based Security Model (USM) for SNMP version 3 for SNMP message level security.</td>
</tr>
<tr>
<td>des</td>
<td>(Optional) Specifies the use of the 56-bit Digital Encryption Standard (DES) algorithm for encryption.</td>
</tr>
<tr>
<td>3des</td>
<td>(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.</td>
</tr>
<tr>
<td>aes</td>
<td>(Optional) Specifies the use of the Advanced Encryption Standard (AES) algorithm for encryption.</td>
</tr>
<tr>
<td>128</td>
<td>(Optional) Specifies the use of a 128-bit AES algorithm for encryption.</td>
</tr>
<tr>
<td>192</td>
<td>(Optional) Specifies the use of a 192-bit AES algorithm for encryption.</td>
</tr>
<tr>
<td>256</td>
<td>(Optional) Specifies the use of a 256-bit AES algorithm for encryption.</td>
</tr>
<tr>
<td>privpassword</td>
<td>(Optional) String (not to exceed 64 characters) that specifies the privacy user password.</td>
</tr>
<tr>
<td>acl-number</td>
<td>(Optional) Integer in the range from 1 to 99 that specifies a standard access list of IP addresses.</td>
</tr>
<tr>
<td>acl-name</td>
<td>(Optional) String (not to exceed 64 characters) that is the name of a standard access list of IP addresses.</td>
</tr>
</tbody>
</table>

**Command Default**

See the table in the “Usage Guidelines” section for default behaviors for encryption, passwords, and access lists.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To configure a remote user, specify the IP address or port number for the remote SNMP agent of the device where the user resides. Also, before you configure remote users for a particular agent, configure the SNMP engine ID, using the `snmp-server engineID` command with the `remote` keyword. The remote agent’s SNMP engine ID is needed when computing the authentication and privacy digests from the password. If the remote engine ID is not configured first, the configuration command will fail.

For the `privpassword` and `auth-password` arguments, the minimum length is one character; the recommended length is at least eight characters, and should include both letters and numbers. The recommended maximum length is 64 characters.

The table below describes the default user characteristics for encryption, passwords, and access lists.
Table 100: snmp-server user Default Descriptions

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access lists</td>
<td>Access from all IP access lists is permitted.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Not present by default. The encrypted keyword is used to specify that the passwords are message digest algorithm 5 (MD5) digests and not text passwords.</td>
</tr>
<tr>
<td>Passwords</td>
<td>Assumed to be text strings.</td>
</tr>
<tr>
<td>Remote users</td>
<td>All users are assumed to be local to this SNMP engine unless you specify they are remote with the remote keyword.</td>
</tr>
</tbody>
</table>

SNMP passwords are localized using the SNMP engine ID of the authoritative SNMP engine. For informs, the authoritative SNMP agent is the remote agent. You need to configure the remote agent’s SNMP engine ID in the SNMP database before you can send proxy requests or informs to it.

Note
Changing the engine ID after configuring the SNMP user, does not allow to remove the user. To remove the user, you need to first reconfigure the SNMP user.

Working with Passwords and Digests

No default values exist for authentication or privacy algorithms when you configure the command. Also, no default passwords exist. The minimum length for a password is one character, although Cisco recommends using at least eight characters for security. The recommended maximum length of a password is 64 characters. If you forget a password, you cannot recover it and will need to reconfigure the user. You can specify either a plain-text password or a localized MD5 digest.

If you have the localized MD5 or Secure Hash Algorithm (SHA) digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

Examples

The following example shows how to add the user abcd to the SNMP server group named public. In this example, no access list is specified for the user, so the standard named access list applied to the group applies to the user.

Device(config)# snmp-server user abcd public v2c

The following example shows how to add the user abcd to the SNMP server group named public. In this example, access rules from the standard named access list qrst apply to the user.

Device(config)# snmp-server user abcd public v2c access qrst

In the following example, the plain-text password cisco123 is configured for the user abcd in the SNMP server group named public:

Device(config)# snmp-server user abcd public v3 auth md5 cisco123
When you enter a `show running-config` command, a line for this user will be displayed. To learn if this user has been added to the configuration, use the `show snmp user` command.

**Note**

The `show running-config` command does not display any of the active SNMP users created in authPriv or authNoPriv mode, though it does display the users created in noAuthNoPriv mode. To display any active SNMPv3 users created in authPriv, authNoPrv, or noAuthNoPriv mode, use the `show snmp user` command.

If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd where aa, bb, and cc are hexadecimal values. Also, the digest should be exactly 16 octets long.

In the following example, the MD5 digest string is used instead of the plain-text password:

```
```

In the following example, the user abcd is removed from the SNMP server group named public:

```
Device(config)# no snmp-server user abcd public v2c
```

In the following example, the user abcd from the SNMP server group named public specifies the use of the 168-bit 3DES algorithm for privacy encryption with `secure3des` as the password:

```
Device(config)# snmp-server user abcd public priv v2c 3des secure3des
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information.</td>
</tr>
<tr>
<td><code>show snmp user</code></td>
<td>Displays information on each SNMP username in the group username table.</td>
</tr>
<tr>
<td><code>snmp-server engineID</code></td>
<td>Displays the identification of the local SNMP engine and all remote engines that have been configured on the device.</td>
</tr>
</tbody>
</table>
snmp-server view

To create or update a view entry, use the snmp-server view command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the no form of this command.

```
no snmp-server view view-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>view-name</code></td>
<td>Label for the view record that you are updating or creating. The name is used to reference the record.</td>
</tr>
<tr>
<td><code>oid-tree</code></td>
<td>Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (<em>) wildcard to specify a subtree family; for example 1.3.</em>.4.</td>
</tr>
<tr>
<td><code>included</code></td>
<td>Configures the OID (and subtree OIDs) specified in <code>oid-tree</code> argument to be included in the SNMP view.</td>
</tr>
<tr>
<td><code>excluded</code></td>
<td>Configures the OID (and subtree OIDs) specified in <code>oid-tree</code> argument to be explicitly excluded from the SNMP view.</td>
</tr>
</tbody>
</table>

**Command Default**

No view entry exists.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.8.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Other SNMP commands require an SNMP view as an argument. You use this command to create a view to be used as arguments for other commands.

Two standard predefined views can be used when a view is required, instead of defining a view. One is `everything`, which indicates that the user can see all objects. The other is `restricted`, which indicates that the user can see three groups: system, snmpStats, and snmpParties. The predefined views are described in RFC 1447.

The first snmp-server command that you enter enables SNMP on your routing device.

**Examples**

The following example creates a view that includes all objects in the MIB-II subtree:

```
snmp-server view mib2 mib-2 included
```

The following example creates a view that includes all objects in the MIB-II system group and all objects in the Cisco enterprise MIB:
The following example creates a view that includes all objects in the MIB-II system group except for sysServices (System 7) and all objects for interface 1 in the MIB-II interfaces group:

```
snmp-server view agon system included
snmp-server view agon system.7 excluded
snmp-server view agon ifEntry.*.1 included
```

In the following example, the USM, VACM, and Community MIBs are explicitly included in the view “test” with all other MIBs under the root parent “internet”:

```
! -- include all MIBs under the parent tree “internet”
snmp-server view test internet included
! -- include snmpUsmMIB
snmp-server view test 1.3.6.1.6.3.15 included
! -- include snmpVacmMIB
snmp-server view test 1.3.6.1.6.3.16 included
! -- exclude snmpCommunityMIB
snmp-server view test 1.3.6.1.6.3.18 excluded
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>snmp-server community</code></td>
<td>Sets up the community access string to permit access to the SNMP protocol.</td>
</tr>
<tr>
<td><code>snmp-server manager</code></td>
<td>Starts the SNMP manager process.</td>
</tr>
</tbody>
</table>

---

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**
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**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface type number</td>
<td>Specifies an interface type and number.</td>
</tr>
<tr>
<td>vlan vlan-ID</td>
<td>Associates the ERSPAN source session number with VLANs. Valid values are from 1 to 4094.</td>
</tr>
<tr>
<td>,</td>
<td>(Optional) Specifies another interface.</td>
</tr>
<tr>
<td>-</td>
<td>(Optional) Specifies a range of interfaces.</td>
</tr>
<tr>
<td>both</td>
<td>(Optional) Monitors both received and transmitted ERSPAN traffic.</td>
</tr>
<tr>
<td>rx</td>
<td>(Optional) Monitors only received traffic.</td>
</tr>
<tr>
<td>tx</td>
<td>(Optional) Monitors only transmitted traffic.</td>
</tr>
</tbody>
</table>

**Command Default**

Source interface or VLAN is not configured.

**Command Modes**

ERSPAN monitor source session configuration mode (config-mon-erspan-src)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```
Device(config)# monitor session 2 type erspan-source
Device(config-mon-erspan-src)# source interface fastethernet 0/1 rx
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitor session type</td>
<td>Configures a local ERSPAN source or destination session.</td>
</tr>
</tbody>
</table>
**switchport mode access**

To set 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 vlan_id`: Specifies to forward all voice traffic through the specified VLAN.

**Command Default**

You can specify a value from 1 to 4094.

**Command Modes**

Template configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to specify to forward all voice traffic through the specified VLAN.

```
Device(config-template)# switchport voice vlan 20
```
switchport voice vlan
PART IX

QoS

• QoS Commands, on page 945
QoS Commands

- auto qos classify, on page 946
- auto qos trust, on page 948
- auto qos video, on page 955
- auto qos voip, on page 965
- class, on page 979
- class-map, on page 981
- debug auto qos, on page 983
- match (class-map configuration), on page 984
- policy-map, on page 988
- priority, on page 990
- queue-buffers ratio, on page 992
- queue-limit, on page 993
- random-detect cos, on page 995
- random-detect cos-based, on page 996
- random-detect dscp, on page 997
- random-detect dscp-based, on page 999
- random-detect precedence, on page 1000
- random-detect precedence-based, on page 1002
- service-policy (Wired), on page 1003
- set, on page 1005
- show auto qos, on page 1011
- show class-map, on page 1013
- show platform hardware fed switch, on page 1014
- show platform software fed switch qos, on page 1018
- show platform software fed switch qos qsb, on page 1019
- show policy-map, on page 1022
- show tech-support qos, on page 1024
- trust device, on page 1026
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.

```plaintext
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**
  - Cisco IOS XE Everest 16.5.1a
  - 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.

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:

You can verify your settings by entering the `show auto qos interface interface-id` privileged EXEC command.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**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 101: Traffic Types, Packet Labels, and Queues**

<table>
<thead>
<tr>
<th></th>
<th>VOIP Data Traffic</th>
<th>VOIP Control Traffic</th>
<th>Routing Protocol Traffic</th>
<th>STP(^1) BPDU(^2) Traffic</th>
<th>Real-Time Video Traffic</th>
<th>All Other Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP(^2)</td>
<td>46</td>
<td>24, 26</td>
<td>48</td>
<td>56</td>
<td>34</td>
<td>–</td>
</tr>
<tr>
<td>CoS(^4)</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>–</td>
</tr>
</tbody>
</table>

1. STP = Spanning Tree Protocol
2. BPDU = bridge protocol data unit
3. DSCP = Differentiated Services Code Point
4. CoS = class of service
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 hundredgigabitethernet1/0/17
Device(config-if)# auto qos trust cos
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/17

Hundredgigabitethernet1/0/17

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
This example shows how to enable auto-QoS for a trusted interface with specific DSCP classification.

Device(config)# interface hundredgigabitethernet1/0/19
Device(config-if)# auto qos trust dscp
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/19

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
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
(totals 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
(totals 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
(totals 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
(totals 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 102: Traffic Types, Packet Labels, and Queues

<table>
<thead>
<tr>
<th></th>
<th>VOIP Data Traffic</th>
<th>VOIP Control Traffic</th>
<th>Routing Protocol Traffic</th>
<th>STP BPDU Traffic</th>
<th>Real-Time Video Traffic</th>
<th>All Other Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSCP(^5)</td>
<td>46</td>
<td>24, 26</td>
<td>48</td>
<td>56</td>
<td>34</td>
<td>–</td>
</tr>
<tr>
<td>CoS(^8)</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>7</td>
<td>3</td>
<td>–</td>
</tr>
</tbody>
</table>

\(^5\) STP = Spanning Tree Protocol
\(^6\) BPDU = bridge protocol data unit
\(^7\) DSCP = Differentiated Services Code Point
\(^8\) CoS = class of service

### Examples

The following is an example of the `auto qos video cts` command and the applied policies and class maps:

```
Device(config)# interface hundredgigabitethernet1/0/13
Device(config-if)# auto qos video cts
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/13
Hundredgigabitethernet1/0/13
```
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
The following is an example of the `auto qos video ip-camera` command and the applied policies and class maps:

```
Device(config)# interface hundredgigabitethernet1/0/9
Device(config-if)# auto qos video ip-camera
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/9

Hundredgigabitethernet1/0/9

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)
The following is an example of the `auto qos video media-player` command and the applied policies and class maps.

```
Device(config)# interface hundredgigabitethernet1/0/7
Device(config-if)# auto qos video media-player
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/7

interface hundredgigabitethernet1/0/7

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
Queueing
  (total drops) 0
  (bytes output) 0
  bandwidth remaining 10%
  queue-buffers ratio 10

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 History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
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.

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-Scavanger-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)
Auto-QoS-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 103: Auto-QoS Configuration for the Egress Queues**

<table>
<thead>
<tr>
<th>Egress Queue</th>
<th>Queue Number</th>
<th>CoS-to-Queue Map</th>
<th>Queue Weight (Bandwidth)</th>
<th>Queue (Buffer) Size for Gigabit-Capable Ports</th>
<th>Queue (Buffer) Size for 10/100 Ethernet Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority (shaped)</td>
<td>1</td>
<td>4, 5</td>
<td>Up to 100 percent</td>
<td>25 percent</td>
<td>15 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>2</td>
<td>2, 3, 6, 7</td>
<td>10 percent</td>
<td>25 percent</td>
<td>25 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>3</td>
<td>0</td>
<td>60 percent</td>
<td>25 percent</td>
<td>40 percent</td>
</tr>
<tr>
<td>SRR shared</td>
<td>4</td>
<td>1</td>
<td>20 percent</td>
<td>25 percent</td>
<td>20 percent</td>
</tr>
</tbody>
</table>

**Examples**

The following is an example of the `auto qos voip trust` command and the applied policies and class maps:

```markdown
Device(config)# interface hundredgigabitethernet1/0/31
Device(config-if)# auto qos voip trust
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/31

**Hundredgigabitethernet1/0/31**

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 hundredgigabitethernet1/0/5
Device(config-if)# auto qos voip cisco-phone
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/5

Hundredgigabitethernet1/0/5

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
```
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 hundredgigabitethernet1/0/21
Device(config-if)# auto qos voip cisco-softphone
Device(config-if)# end
Device# show policy-map interface hundredgigabitethernet1/0/21

Hundredgigabitethernet1/0/21

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-Scavenger-Class (match-any)
  0 packets
  Match: access-group name AutoQos-4.0-Acl-Scavenger
    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.
**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}
noclass {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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 the **set** command.
- **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` and polices the traffic at an average rate of 1 Mb/s and bursts at 1000 bytes, marking down exceeding traffic via a table-map.

```
Device(config)# policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# police cir 1000000 bc 1000 conform-action
transmit exceed-action set-dscp-transmit dscp table EXEC_TABLE
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 criteria must match.
- **class-map-name**  The class map name.

**Command Default**
No class maps are defined.

**Command Modes**
Global configuration
Policy map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to specify the name of the class for which you want to create or modify class-map match criteria and to enter class-map configuration mode.

The class-map command and its subcommands are used to define packet classification, marking, and aggregate policing as part of a globally named service policy applied on a per-port basis.

After you are in quality of service (QoS) class-map configuration mode, these configuration commands are available:

- **description**—Describes the class map (up to 200 characters). The show class-map privileged EXEC command displays the description and the name of the class map.
- **exit**—Exits from QoS class-map configuration mode.
- **match**—Configures classification criteria.
- **no**—Removes a match statement from a class map.

If you enter the match-any keyword, you can only use it to specify an extended named access control list (ACL) with the match access-group class-map configuration command.

To define packet classification on a physical-port basis, only one match command per class map is supported. The ACL can have multiple access control entries (ACEs).
This example shows how to configure the class map called class1 with one match criterion, which is an access list called 103:

```
Device(config)# access-list 103 permit ip any any dscp 10
Device(config)# class-map class1
Device(config-cmap)# match access-group 103
Device(config-cmap)# exit
```

This example shows how to delete the class map class1:

```
Device(config)# no class-map class1
```

You can verify your settings by entering the `show class-map` privileged EXEC command.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 hundredgigabitethernet 1/0/3
Device(config-if)# auto qos voip cisco-phone
```
**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.

**Cisco IOS XE Everest 16.5.x and Earlier Releases**

```plaintext
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 }
```

**Cisco IOS XE Everest 16.6.x and Later Releases**

```plaintext
match { access-group { name acl-name acl-index } | cos cos-value | dscp dscp-value | [ ip ] dscp dscp-list | [ ip ] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id }
no match { access-group { name acl-name acl-index } | cos cos-value | dscp dscp-value | [ ip ] dscp dscp-list | [ ip ] precedence ip-precedence-list | mpls experimental-value | non-client-nrt | precedence precedence-value1...value4 | protocol protocol-name | qos-group qos-group-value | vlan vlan-id | wlan wlan-id }
```

### Syntax Description

<table>
<thead>
<tr>
<th>access-group</th>
<th>Specifies an access group.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name acl-name</td>
<td>Specifies the name of an IP standard or extended access control list (ACL) or MAC ACL.</td>
</tr>
<tr>
<td>acl-index</td>
<td>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.</td>
</tr>
<tr>
<td>class-map class-map-name</td>
<td>Uses a traffic class as a classification policy and specifies a traffic class name to use as the match criterion.</td>
</tr>
<tr>
<td>cos cos-value</td>
<td>Matches a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking. The cos-value is from 0 to 7. You can specify up to four CoS values in one <code>match cos</code> statement, separated by a space.</td>
</tr>
<tr>
<td>dscp dscp-value</td>
<td>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.</td>
</tr>
</tbody>
</table>
### match (class-map configuration)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip dscp</strong> dscp-list</td>
<td>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.</td>
</tr>
<tr>
<td><strong>ip precedence</strong> ip-precedence-list</td>
<td>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.</td>
</tr>
<tr>
<td><strong>precedence</strong> precedence-value1...value4</td>
<td>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.</td>
</tr>
<tr>
<td><strong>qos-group</strong> qos-group-value</td>
<td>Identifies a specific QoS group value as a match criterion. The range is 0 to 31.</td>
</tr>
<tr>
<td><strong>vlan</strong> vlan-id</td>
<td>Identifies a specific VLAN as a match criterion. The range is 1 to 4094.</td>
</tr>
<tr>
<td><strong>mpls</strong> experimental-value</td>
<td>Specifies Multi Protocol Label Switching specific values.</td>
</tr>
<tr>
<td><strong>non-client-nrt</strong></td>
<td>Matches a non-client NRT (non-real-time).</td>
</tr>
<tr>
<td><strong>protocol</strong> protocol-name</td>
<td>Specifies the type of protocol.</td>
</tr>
<tr>
<td><strong>wlan</strong> wlan-id</td>
<td>Identifies 802.11 specific values.</td>
</tr>
</tbody>
</table>

**Command Default**

No match criteria are defined.

**Command Modes**

Class-map configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>The class-map class-map-name keyword is removed. The mpls experimental-value, non-client-nrt, protocol protocol-name, and wlan wlan-id keywords are added.</td>
</tr>
</tbody>
</table>

**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**
The ACL must be an extended named ACL.

This is not applicable to Cisco Catalyst 9500 Series High Performance Switches.

- **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.
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**
  - Cisco IOS XE Everest 16.5.1a

  **Modification**
  - 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.

**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 shows you how to configure hierarchical policies:

```
Device(config)# 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-policy)# 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.

```
```

**Syntax Description**

- **Kbps** (Optional) Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps.

- **burst -in-bytes** (Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.

- **level level-value** (Optional) Assigns priority level. Available values for `level-value` are 1 and 2. Level 1 is a higher priority than Level 2. Level 1 reserves bandwidth and goes first, so latency is very low.

- **percent percentage** (Optional) Specifies the amount of guaranteed bandwidth to be specified by the percent of available bandwidth.

**Command Default**

No priority is set.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

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.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.
Example

The following example shows how to configure the priority of the class in policy map policy1:

```
Device(config)# class-map cm1
Device(config-cmap)# match precedence 2
Device(config-cmap)# exit

Device(config)# class-map cm2
Device(config-cmap)# match dscp 30
Device(config-cmap)# exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm1
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 1m
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit
Device(config-pmap)# exit

Device(config)# policy-map policy1
Device(config-pmap)# class cm2
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 1m
```
queue-buffers ratio

To configure the queue buffer for the class, use the **queue-buffers ratio** command in policy-map class configuration mode. Use the **no** form of this command to remove the ratio limit.

**queue-buffers ratio**  **ratio limit**
**no queue-buffers ratio**  **ratio limit**

**Syntax Description**

- **ratio limit**  (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0-100).

**Command Default**
No queue buffer for the class is defined.

**Command Modes**
Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Either the **bandwidth**, **shape**, or **priority** command must be used before using this command. For more information about these commands, see *Cisco IOS Quality of Service Solutions Command Reference* available on Cisco.com.

The device 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.

**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-c)#  end
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.
queue-limit

To specify or modify the maximum number of packets the queue can hold for a class policy configured in a policy map, use the `queue-limit` policy-map class configuration command. To remove the queue packet limit from a class, use the `no` form of this command.

```
queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent percentage-of-packets
no queue-limit queue-limit-size [{packets}] {cos cos-value | dscp dscp-value} percent percentage-of-packets
```

**Syntax Description**

- `queue-limit-size` The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (bytes, ms, us, or packets).
- `cos cos-value` Specifies parameters for each CoS value. CoS values are from 0 to 7.
- `dscp dscp-value` Specifies parameters for each DSCP value. You can specify a value in the range 0 to 63 specifying the differentiated services code point value for the type of queue limit.
- `percent percentage-of-packets` A percentage in the range 1 to 100 specifying the maximum percentage of packets that the queue for this class can accumulate.

**Command Default**

None

**Command Modes**

Policy-map class configuration (policy-map-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 policy1
Device(config-pmap)# class dscp-1
Device(config-pmap-c)# bandwidth percent 20
Device(config-pmap-c)# queue-limit dscp 1 percent 20
```
random-detect cos

To change the minimum and maximum packet thresholds for the Class of service (CoS) value, use the `random-detect cos` command in QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the CoS value, use the `no` form of this command.

```
random-detect cos cos-value percent min-threshold max-threshold
no random-detect cos cos-value percent min-threshold max-threshold
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cos-value</code></td>
<td>The CoS value, which is IEEE 802.1Q/ISL class of service/user priority value. The CoS value can be a number from 0 to 7.</td>
<td></td>
</tr>
<tr>
<td><code>percent</code></td>
<td>Specifies that the minimum and threshold values are in percentage.</td>
<td></td>
</tr>
<tr>
<td><code>min-threshold</code></td>
<td>Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified CoS value.</td>
<td></td>
</tr>
<tr>
<td><code>max-threshold</code></td>
<td>Maximum threshold in number of packets. The value range of this argument is from the value of the <code>min-threshold</code> argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified CoS value.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

QoS policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `random-detect cos` command in conjunction with the `random-detect` command in QoS policy-map class configuration mode.

The `random-detect cos` command is available only if you have specified the `cos-based` argument when using the `random-detect` command in interface configuration mode.

**Examples**

The following example enables WRED to use the CoS value 8. The minimum threshold for the CoS value 8 is 20, the maximum threshold is 40.

```
random-detect cos-based
random-detect cos percent 5 20 40
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>random-detect</code></td>
<td>Enables WRED</td>
</tr>
</tbody>
</table>
**random-detect cos-based**

To enable weighted random early detection (WRED) on the basis of the class of service (CoS) value of a packet, use the `random-detect cos-based` command in policy-map class configuration mode. To disable WRED, use the `no` form of this command.

```
random-detect cos-based
no random-detect cos-based
```

**Command Default**

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

In the following example, WRED is configured on the basis of the CoS value.

```
Device> enable
Device# configure terminal
Device(config)# policy-map policymap1
Device(config-pmap)# class class1
Device(config-pmap-c)# random-detect cos-based
Device(config-pmap-c)#
end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>random-detect cos</code></td>
<td>Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED.</td>
</tr>
<tr>
<td><code>show policy-map</code></td>
<td>Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.</td>
</tr>
<tr>
<td><code>show policy-map interface</code></td>
<td>Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.</td>
</tr>
</tbody>
</table>
random-detect dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the random-detect dscp command in QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the no form of this command.

```
rando\nd\ndetect dscp  dscp-value  percent  min-threshold  max-threshold
no  random-detect dscp  dscp-value  percent  min-threshold  max-threshold
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dscp-value</td>
<td>The DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs7, ef, or rsvp.</td>
</tr>
<tr>
<td>percent</td>
<td>Specifies that the minimum and threshold values are in percentage.</td>
</tr>
<tr>
<td>min-threshold</td>
<td>Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drop some packets with the specified DSCP value.</td>
</tr>
<tr>
<td>max-threshold</td>
<td>Maximum threshold in number of packets. The value range of this argument is from the value of the min-threshold argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified DSCP value.</td>
</tr>
</tbody>
</table>

**Command Modes**

QoS policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the random-detect dscp command in conjunction with the random-detect command in QoS policy-map class configuration mode.

The random-detect dscp command is available only if you specified the dscp-based argument when using the random-detect command in interface configuration mode.

**Specifying the DSCP Value**

The random-detect dscp command allows you to specify the DSCP value per traffic class. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs7, ef, or rsvp.

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 Assured Forwarding (AF) code points, 1 Expedited Forwarding code point, and 8 user-defined DSCP values.
Assured Forwarding Code Points

The AF code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the DSCP value determine the AF class; the lower three values determine the drop probability.

Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

`random-detect dscp percent 8 20 40`

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>random-detect</td>
<td>Enables WRED</td>
</tr>
</tbody>
</table>
random-detect dscp-based

To base weighted random early detection (WRED) on the Differentiated Services Code Point (dscp) value of a packet, use the random-detect dscp-based command in policy-map class configuration mode. To disable this feature, use the no form of this command.

random-detect dscp-based
no random-detect dscp-based

Syntax Description
This command has no arguments or keywords.

Command Default
WRED is disabled by default.

Command Modes
Policy-map class configuration (config-pmap-c)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
With the random-detect dscp-based command, WRED is based on the dscp value of the packet. Use the random-detect dscp-based command before configuring the random-detect dscp command.

Examples
The following example shows that random detect is based on the precedence value of a packet:

```
Device> enable
Device# configure terminal
Device(config)#

policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# random-detect dscp-based
Device(config-pmap-c)# random-detect dscp 2 percent 10 40
Device(config-pmap-c)# exit
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>random-detect</td>
<td>Enables WRED.</td>
</tr>
<tr>
<td>random-detect dscp</td>
<td>Configures the WRED parameters for a particular DSCP value for a class policy in a policy map.</td>
</tr>
</tbody>
</table>
### random-detect precedence

To configure Weighted Random Early Detection (WRED) parameters for a particular IP precedence for a class policy in a policy map, use the `random-detect precedence` command in QoS policy-map class configuration mode. To return the values to the default for the precedence, use the `no` form of this command.

```
random-detect precedence precedence percent min-threshold max-threshold
no random-detect precedence
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>precedence</code></td>
<td>IP precedence number. The value range is from 0 to 7; see Table 1 in the “Usage Guidelines” section.</td>
</tr>
<tr>
<td><code>percent</code></td>
<td>Indicates that the threshold values are in percentage.</td>
</tr>
<tr>
<td><code>min-threshold</code></td>
<td>Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.</td>
</tr>
<tr>
<td><code>max-threshold</code></td>
<td>Maximum threshold in number of packets. The value range of this argument is from the value of the <code>min-threshold</code> argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified IP precedence.</td>
</tr>
</tbody>
</table>

**Command Default**

The default `min-threshold` value depends on the precedence. The `min-threshold` value for IP precedence 0 corresponds to half of the `max-threshold` value. The values for the remaining precedences fall between half the `max-threshold` value and the `max-threshold` value at evenly spaced intervals. See the table in the “Usage Guidelines” section of this command for a list of the default minimum threshold values for each IP precedence.

**Command Modes**

- Interface configuration (config-if)
- QoS policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists.

When you configure the `random-detect` command on an interface, packets are given preferential treatment based on the IP precedence of the packet. Use the `random-detect precedence` command to adjust the treatment for different precedences.

If you want WRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use appropriate values for the minimum and maximum thresholds.

Note that if you use the `random-detect precedence` command to adjust the treatment for different precedences within class policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.
Although the range of values for the `min-threshold` and `max-threshold` arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.

Examples

The following example shows the configuration to enable WRED on the interface and to specify parameters for the different IP precedences:

```plaintext
interface FortyGigE1/0/1
description 45Mbps to R1
ip address 10.200.14.250 255.255.255.252
random-detect
random-detect precedence 7 percent 20 50
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bandwidth (policy-map class)</code></td>
<td>Specifies or modifies the bandwidth allocated for a class belonging to a policy map.</td>
</tr>
<tr>
<td><code>random-detect dscp</code></td>
<td>Changes the minimum and maximum packet thresholds for the DSCP value.</td>
</tr>
<tr>
<td><code>show policy-map interface</code></td>
<td>Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.</td>
</tr>
<tr>
<td><code>show queuing</code></td>
<td>Lists all or selected configured queuing strategies.</td>
</tr>
</tbody>
</table>
random-detect precedence-based

To base weighted random early detection (WRED) on the precedence value of a packet, use the `random-detect precedence-based` command in policy-map class configuration mode. To disable this feature, use the `no` form of this command.

```
random-detect precedence-based
no random-detect precedence-based
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

WRED is disabled by default.

**Command Modes**

Policy-map class configuration (config-pmap-c)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

With the `random-detect precedence-based` command, WRED is based on the IP precedence value of the packet.

Use the `random-detect precedence-based` command before configuring the `random-detect precedence-based` command.

**Examples**

The following example shows that random detect is based on the precedence value of a packet:

```
Device> enable
Device# configure terminal
Device(config)#

policy-map policy1
Device(config-pmap)# class class1
Device(config-pmap-c)# bandwidth percent 80
Device(config-pmap-c)# random-detect precedence-based
Device(config-pmap-c)# random-detect precedence 2 percent 30 50
Device(config-pmap-c)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>random-detect</td>
<td>Enables WRED.</td>
</tr>
<tr>
<td>random-detect precedence</td>
<td>Configures the WRED parameters for a particular IP precedence for a class policy in a policy map.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Examples**

This example shows how to apply plcmap1 to an physical ingress port:

```
Device(config)# interface hundredgigabitethernet 1/0/3
Device(config-if)# service-policy input plcmap1
```

This example shows how to remove plcmap2 from a physical port:

```
Device(config)# interface hundredgigabitethernet 1/0/5
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-policy)# end
Device# configure terminal
```
Device(config)# interface hundredgigabitethernet 1/0/5
Device(config-if)# service-policy input vlan100

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 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` (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 Everest 16.5.1a 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.

**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
Hundredgigabitethernet 1/0/3
  auto qos voip cisco-softphone
Hundredgigabitethernet 1/0/5
  auto qos voip cisco-phone
Hundredgigabitethernet 1/0/7
  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 Hundredgigabitethernet 1/0/5
Hundredgigabitethernet 1/0/5
  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 Hundredgigabitethernet 1/0/11
```
AutoQoS is disabled
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 | [{aqmreppqostbl | iqslabeltable | sqslabeltable}] | {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.

**Note**

The switch keyword is now optional on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>afd { config type</td>
<td>stats client }</td>
</tr>
<tr>
<td>config type:</td>
<td><strong>client</strong>—Displays wireless client information</td>
</tr>
<tr>
<td></td>
<td><strong>port</strong>—Displays port-specific information</td>
</tr>
<tr>
<td></td>
<td><strong>radio</strong>—Displays wireless radio information</td>
</tr>
<tr>
<td></td>
<td><strong>ssid</strong>—Displays wireless SSID information</td>
</tr>
<tr>
<td>stats client:</td>
<td><strong>all</strong>—Displays statistics of all client.</td>
</tr>
<tr>
<td></td>
<td><strong>bssid</strong>—Valid range is from 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td><strong>wlanid</strong>—Valid range is from 1 to 4294967295</td>
</tr>
<tr>
<td>asicasic_num</td>
<td>(Optional) ASIC number. Valid range is from 0 to 255.</td>
</tr>
<tr>
<td>dscp-cos counters</td>
<td>Displays per port dscp-cos counters. You must choose from the following options under <strong>dscp-cos counters</strong>:</td>
</tr>
<tr>
<td>iif_id id</td>
<td>interface type number }</td>
</tr>
<tr>
<td></td>
<td><strong>interface type number</strong>—Target interface type and ID.</td>
</tr>
<tr>
<td>leinfo</td>
<td>You must choose from the following options under <strong>dscp-cos counters</strong>:</td>
</tr>
<tr>
<td></td>
<td><strong>iif_id id</strong>—The target interface ID. Valid range is from 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td><strong>interface type number</strong>—Target interface type and ID.</td>
</tr>
<tr>
<td>policer config</td>
<td>Displays configuration information related to policers in hardware. You must choose from the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>iif_id id</strong>—The target interface ID. Valid range is from 1 to 4294967295.</td>
</tr>
<tr>
<td></td>
<td><strong>interface type number</strong>—Target interface type and ID.</td>
</tr>
</tbody>
</table>
queue \{ \texttt{config} (iif\_id id | \texttt{interface} type number | \texttt{internal}) | \texttt{label2qmap} | \texttt{stats} \} \texttt{stats} \texttt{internal cpu policer} \texttt{switch\_number} \texttt{qos queue stats} \texttt{internal cpu policer} \texttt{command}

<table>
<thead>
<tr>
<th>QId</th>
<th>PlcIdx</th>
<th>Queue Name</th>
<th>Enabled</th>
<th>(default) Rate</th>
<th>(set) Rate</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>11</td>
<td>DOT1X Auth</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>L2 Control</td>
<td>No</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>Forus traffic</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>ICMP GEN</td>
<td>Yes</td>
<td>200</td>
<td>200</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>Routing Control</td>
<td>Yes</td>
<td>1800</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>14</td>
<td>Forus Address resolution</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>3</td>
<td>ICMP Redirect</td>
<td>No</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>WLESS PRI-5</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
</tbody>
</table>

This is an example of output from the `show platform hardware fed switch \texttt{switch\_number} qos queue stats \texttt{internal cpu policer}` command.
<table>
<thead>
<tr>
<th>No</th>
<th>Feature</th>
<th>Value</th>
<th>Buffer Size</th>
<th>MTU</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>WLESS PRI-1</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>WLESS PRI-2</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>WLESS PRI-3</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>WLESS PRI-4</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>BROADCAST</td>
<td>Yes</td>
<td>200</td>
<td>200</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>Learning cache ovfl</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>Sw forwarding</td>
<td>Yes</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>Topology Control</td>
<td>No</td>
<td>13000</td>
<td>13000</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>Proto Snooping</td>
<td>No</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>DHCP Snooping</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>Transit Traffic</td>
<td>Yes</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>RPF Failed</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>MCAST END STATION</td>
<td>Yes</td>
<td>2000</td>
<td>2000</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>LOGGING</td>
<td>Yes</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>Punt Webauth</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>Crypto Control</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>Exception</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>General Punt</td>
<td>No</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>NFL SAMPLED DATA</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>27</td>
<td>SGT Cache Full</td>
<td>Yes</td>
<td>1800</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>EGR Exception</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>Show frwd</td>
<td>No</td>
<td>1000</td>
<td>1000</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>MCAST Data</td>
<td>Yes</td>
<td>500</td>
<td>500</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>Gold Pkt</td>
<td>Yes</td>
<td>100</td>
<td>100</td>
<td>0</td>
</tr>
</tbody>
</table>
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 of 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.
  - `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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.

### Note

This command is not supported on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

**show platform software fed switch**

- **switch_number**: 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.
show platform software fed switch qos qsb

| Command Modes | User EXEC  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

| Command History | Cisco IOS XE Everest 16.5.1a  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Note: This command is not supported on the C9500-32C, C9500-32QC, C9500-48Y4C, and C9500-24Y4C models of the Cisco Catalyst 9500 Series Switches.

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)
Policy 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.

```plaintext
show policy-map [{policy-map-name | interface interface-id}]
```

**Syntax Description**
- `policy-map-name` (Optional) Name of the policy-map.
- `interface interface-id` (Optional) Displays the statistics and the configurations of the input and output policies that are attached to the interface.

**Command Modes**
- User EXEC
- Privileged EXEC

**Command History**
- Release: Cisco IOS XE Everest 16.5.1a
- Modification: This command was introduced.

**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 TwentyFiveGigE 1/0/47

Service-policy output: port_shape_parent

Class-map: class-default (match-any)
  191509734 packets
  Match: any
  Queueing

  (total drops) 524940551420
  (bytes output) 14937264500
  shape (average) cir 250000000, bc 2500000, be 2500000
  target shape rate 250000000

  Service-policy : child_trip_play

    queue stats for all priority classes:
      Queueing
      priority level 1
```
(total drops) 524940551420
(bytes output) 14937180648

queue stats for all priority classes:
Queueing
priority level 2

(total drops) 0
(bytes output) 0

Class-map: dscp56 (match-any)
191508445 packets
Match: dscp cs7 (56)
0 packets, 0 bytes
5 minute rate 0 bps
Priority: Strict,

Priority Level: 1
police:
  cir 10 %
  cir 25000000 bps, bc 781250 bytes
conformed 0 bytes; actions: >>>>>counters not supported
  transmit
exceeded 0 bytes; actions:
drop
conformed 0000 bps, exceeded 0000 bps >>>>>counters not supported
show tech-support qos

To display quality of service (QoS)-related information for use by technical support, use the `show tech-support qos` command in privileged EXEC mode.

```
show tech-support qos [{switch {switch-number | active | all | standby} | [{control-plane | interface {interface-name | all}}]}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch switch-number</code></td>
<td>(Optional) Displays QoS-related information for a specific switch.</td>
</tr>
<tr>
<td><code>active</code></td>
<td>(Optional) Displays QoS-related information for the active instance of the switch.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays QoS-related information for all instances of the switch.</td>
</tr>
<tr>
<td><code>standby</code></td>
<td>(Optional) Displays QoS-related information for the standby instance of the switch.</td>
</tr>
<tr>
<td><code>control-plane</code></td>
<td>(Optional) Displays QoS-related information for the control-plane.</td>
</tr>
<tr>
<td><code>interface interface-name</code></td>
<td>(Optional) Displays QoS-related information for a specified interface.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>(Optional) Displays QoS-related information for all interfaces.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support qos | redirect flash: filename`) in the local writable storage file system or remote file system.

The output of the `show tech-support qos` command displays a list of commands and their output. These commands differ based on the platform.

**Examples**

The following is sample output from the `show tech-support qos` command:

```
Device# show tech-support qos
```


## TCG summary for policy: system-cpp-policy

<table>
<thead>
<tr>
<th>Loc</th>
<th>Interface</th>
<th>IIF-ID</th>
<th>Dir</th>
<th>tccg</th>
<th>Child #m/p/q</th>
<th>State: (cfg,opr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7:0</td>
<td>CoPP-Queue-0</td>
<td>0x000000010000000d</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-1</td>
<td>0x000000010000000e</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-2</td>
<td>0x000000010000000f</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-3</td>
<td>0x0000000100000100</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-4</td>
<td>0x0000000100000101</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-5</td>
<td>0x0000000100000102</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-6</td>
<td>0x0000000100000103</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-7</td>
<td>0x0000000100000104</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-8</td>
<td>0x0000000100000105</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-9</td>
<td>0x0000000100000106</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-10</td>
<td>0x0000000100000107</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-11</td>
<td>0x0000000100000108</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-12</td>
<td>0x0000000100000109</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-13</td>
<td>0x000000010000010a</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-14</td>
<td>0x000000010000010b</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-15</td>
<td>0x000000010000010c</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-16</td>
<td>0x000000010000010d</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-17</td>
<td>0x000000010000010e</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-18</td>
<td>0x000000010000010f</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-19</td>
<td>0x0000000100000120</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-20</td>
<td>0x0000000100000121</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-21</td>
<td>0x0000000100000122</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-22</td>
<td>0x0000000100000123</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-23</td>
<td>0x0000000100000124</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-24</td>
<td>0x0000000100000125</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-25</td>
<td>0x0000000100000126</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-26</td>
<td>0x0000000100000200</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-27</td>
<td>0x0000000100000201</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-28</td>
<td>0x0000000100000202</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-29</td>
<td>0x0000000100000203</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-30</td>
<td>0x0000000100000204</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
<tr>
<td>7:0</td>
<td>CoPP-Queue-31</td>
<td>0x0000000100000205</td>
<td>OUT</td>
<td>22</td>
<td>0/0/0/0/0</td>
<td>VALID, SET_INHW</td>
</tr>
</tbody>
</table>

### Policymap Summary: (counters)

| CGID | Classes | Targets | Child CfgErr InHw OpErr Policy Name |
|------|---------|---------|-------------------------------|------------------|
| 15212688 | 22 | 33 | 0 | 0 | 33 | 0 | system-cpp-policy |

Output fields are self-explanatory.
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}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-phone</td>
<td>Configures a Cisco IP phone</td>
</tr>
<tr>
<td>cts</td>
<td>Configures a Cisco TelePresence System</td>
</tr>
<tr>
<td>ip-camera</td>
<td>Configures an IP Video Surveillance Camera (IPVSC)</td>
</tr>
<tr>
<td>media-player</td>
<td>Configures a Cisco Digital Media Player (DMP)</td>
</tr>
</tbody>
</table>

**Command Default**

Trust disabled

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 TwentyFiveGigE 1/0/1:

```
Device(config)# interface TwentyFiveGigE 1/0/1
Device(config-if)# trust device cisco-phone
```
trust device
PART X

Routing

• IP Routing Commands, on page 1031
IP Routing Commands

- address-family ipv6 (OSPF), on page 1033
- aggregate-address, on page 1034
- area nssa, on page 1037
- area virtual-link, on page 1039
- auto-summary (BGP), on page 1042
- authentication (BFD), on page 1045
- bfd, on page 1046
- bfd all-interfaces, on page 1048
- bfd check-ctrl-plane-failure, on page 1049
- bfd echo, on page 1050
- bfd slow-timers, on page 1052
- bfd template, on page 1054
- bfd-template single-hop, on page 1055
- bgp graceful-restart, on page 1056
- clear proximity ip bgp, on page 1058
- default-information originate (OSPF), on page 1062
- default-metric (BGP), on page 1064
- distance (OSPF), on page 1066
- eigrp log-neighbor-changes, on page 1069
- ip authentication key-chain eigrp, on page 1071
- ip authentication mode eigrp, on page 1072
- ip bandwidth-percent eigrp, on page 1073
- ip cef load-sharing algorithm, on page 1074
- ip community-list, on page 1075
- ip prefix-list, on page 1080
- ip hello-interval eigrp, on page 1083
- ip hold-time eigrp, on page 1084
- ip load-sharing, on page 1085
- ip next-hop-self eigrp, on page 1086
- ip ospf database-filter all out, on page 1088
- ip ospf name-lookup, on page 1089
- ip split-horizon eigrp, on page 1090
- ip summary-address eigrp, on page 1091
• ip route static bfd, on page 1093
• ipv6 route static bfd, on page 1095
• metric weights (EIGRP), on page 1096
• neighbor advertisement-interval, on page 1098
• neighbor default-originate, on page 1100
• neighbor description, on page 1102
• neighbor ebgp-multihop, on page 1103
• neighbor maximum-prefix (BGP), on page 1104
• neighbor peer-group (assigning members), on page 1106
• neighbor peer-group (creating), on page 1108
• neighbor route-map, on page 1111
• neighbor update-source, on page 1113
• network (BGP and multiprotocol BGP), on page 1115
• network (EIGRP), on page 1117
• nsf (EIGRP), on page 1119
• offset-list (EIGRP), on page 1121
• router bgp, on page 1123
• router-id, on page 1126
• router eigrp, on page 1127
• redistribute (IPv6), on page 1128
• redistribute maximum-prefix (OSPF), on page 1131
• rewrite-evpn-rt-asn, on page 1133
• router ospf, on page 1134
• router ospfv3, on page 1136
• set community, on page 1137
• set ip next-hop (BGP), on page 1139
• show ip bgp, on page 1141
• show ip bgp neighbors, on page 1153
• show ip eigrp interfaces, on page 1168
• show ip eigrp neighbors, on page 1171
• show ip eigrp topology, on page 1174
• show ip eigrp traffic, on page 1179
• show ip ospf, on page 1181
• show ip ospf border-routers, on page 1189
• show ip ospf database, on page 1190
• show ip ospf interface, on page 1199
• show ip ospf neighbor, on page 1202
• show ip ospf virtual-links, on page 1208
• summary-address (OSPF), on page 1209
• timers throttle spf, on page 1211
address-family ipv6 (OSPF)

To enter the address family configuration mode for configuring routing sessions, such as Open Shortest Path First (OSPF), that uses the standard IPv6 address prefixes, use the `address-family ipv6` command in the router configuration mode. To disable the address family configuration mode, use the `no` form of this command.

```
address-family ipv6 [unicast ][{vrf vrf-name }]
no address-family ipv6 [unicast ][{vrf vrf-name }]
```

**Syntax Description**
- `unicast` (Optional) Specifies the IPv6 unicast address prefixes.
- `vrf` (Optional) Specifies all the VPN routing and forwarding (VRF) instance tables or a specific VRF table for an IPv6 address.
- `vrf-name` (Optional) A specific VRF table for an IPv6 address.

**Command Default**
IPv6 address prefixes are not enabled. Unicast address prefixes are the default when the IPv6 address prefixes are configured.

**Command Modes**
Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `address-family ipv6` command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use the standard IPv6 address prefixes.

**Examples**
The following example shows how to place the router in address family configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router ospfv3</td>
<td>Enters OSPFv3 router configuration mode.</td>
</tr>
</tbody>
</table>
aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the `aggregate-address` command in address family or router configuration mode. To disable this function, use the `no` form of this command.

```
aggregate-address address mask [as-set] [as-confed-set] [summary-only] [suppress-map map-name] [advertise-map map-name] [attribute-map map-name]
no aggregate-address address mask [as-set] [as-confed-set] [summary-only] [suppress-map map-name] [advertise-map map-name] [attribute-map map-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Aggregate address.</td>
</tr>
<tr>
<td>mask</td>
<td>Aggregate mask.</td>
</tr>
<tr>
<td>as-set</td>
<td>(Optional) Generates autonomous system set path information.</td>
</tr>
<tr>
<td>as-confed-set</td>
<td>(Optional) Generates autonomous confederation set path information.</td>
</tr>
<tr>
<td>summary-only</td>
<td>(Optional) Filters all more-specific routes from updates.</td>
</tr>
<tr>
<td>suppress-map map-name</td>
<td>(Optional) Specifies the name of the route map used to select the routes to be suppressed.</td>
</tr>
<tr>
<td>advertise-map map-name</td>
<td>(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.</td>
</tr>
<tr>
<td>attribute-map map-name</td>
<td>(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.</td>
</tr>
</tbody>
</table>

**Command Default**

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the `as-set` keyword is specified.

**Command Modes**

- Address family configuration (config-router-af)
- Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the `aggregate-address` command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute.
set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the as-set keyword.)

Using the as-set keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the aggregate-address command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the as-confed-set keyword creates an aggregate entry using the same rules that the command follows without this keyword. This keyword performs the same function as the as-set keyword, except that it generates autonomous confed set path information.

Using the summary-only keyword not only creates the aggregate route (for example, 192.0.0.0) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the neighbor distribute-list command, with caution. If a more-specific route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the suppress-map keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the match clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the advertise-map keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the aggregate-address command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists match clauses are supported.

Using the attribute-map keyword allows attributes of the aggregate route to be changed. This form of the aggregate-address command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

**AS-Set Example**

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
Device(config)#router bgp 50000
Device(config-router)#aggregate-address 10.0.0.0 255.0.0.0 as-set
```

**Summary-Only Example**

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database under the IP Version 4 address family. Because the summary-only keyword is configured, more-specific routes are filtered from updates.

```
Device(config)#router bgp 50000
```
Conditional Aggregation Example

In the following example, a route map called MAP-ONE is created to match on an AS-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
Device(config)#ip as-path access-list 1 deny ^1234_
Device(config)#ip as-path access-list 1 permit .*
Device(config)#!
Device(config)#route-map MAP-ONE
Device(config-route-map)#match ip as-path 1
Device(config-route-map)#exit
Device(config-router)#router bgp 50000
Device(config-router)#address-family ipv4
Device(config-router-af)#aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map MAP-ONE
Router(config-router-af)#end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 (BGP)</td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td>ip as-path access-list</td>
<td>Defines a BGP autonomous system path access list.</td>
</tr>
<tr>
<td>match ip address</td>
<td>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.</td>
</tr>
<tr>
<td>neighbor distribute-list</td>
<td>Distributes BGP neighbor information in an access list.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
</tbody>
</table>
area nssa

To configure a not-so-stubby area (NSSA), use the `area nssa` command in router address family topology or router configuration mode. To remove the NSSA distinction from the area, use the `no` form of this command.

```
area nssa command
area area-id nssa [no-redistribution] [default-information-originate [metric [metric-type]] [no-summary] [nssa-only]]
o no area area-id nssa [no-redistribution] [default-information-originate [metric [metric-type]] [no-summary] [nssa-only]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>area-id</code></td>
<td>Identifier for the stub area or NSSA. The identifier can be specified as either a decimal value or an IP address.</td>
</tr>
<tr>
<td><code>no-redistribution</code></td>
<td>(Optional) Used when the router is an NSSA Area Border Router (ABR) and you want the <code>redistribute</code> command to import routes only into the normal areas, but not into the NSSA area.</td>
</tr>
<tr>
<td><code>default-information-originate</code></td>
<td>(Optional) Used to generate a Type 7 default into the NSSA area. This keyword takes effect only on the NSSA ABR or the NSSA Autonomous System Boundary Router (ASBR).</td>
</tr>
<tr>
<td><code>metric</code></td>
<td>(Optional) Specifies the OSPF default metric.</td>
</tr>
<tr>
<td><code>metric-type</code></td>
<td>(Optional) Specifies the OSPF metric type for default routes.</td>
</tr>
<tr>
<td><code>no-summary</code></td>
<td>(Optional) Allows an area to be an NSSA but not have summary routes injected into it.</td>
</tr>
<tr>
<td><code>nssa-only</code></td>
<td>(Optional) Limits the default advertisement to this NSSA area by setting the propagate (P) bit in the type-7 LSA to zero.</td>
</tr>
</tbody>
</table>

**Command Default**

No NSSA area is defined.

**Command Modes**

Router address family topology configuration (config-router-af-topology) Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To remove the specified area from the software configuration, use the `no area area-id` command (with no other keywords). That is, the `no area area-id` command removes all area options, including `area authentication`, `area default-cost`, `area nssa`, `area range`, `area stub`, and `area virtual-link`.

**Release 12.2(33)SRB**

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the `area nssa` command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

**Examples**

The following example makes area 1 an NSSA area:
router ospf 1
redistribute rip subnets
network 172.19.92.0 0.0.0.255 area 1
area 1 nssa

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
area virtual-link

To define an Open Shortest Path First (OSPF) virtual link, use the **area virtual-link** command in router address family topology, router configuration, or address family configuration mode. To remove a virtual link, use the **no** form of this command.

```
area area-id virtual-link router-id authentication key-chain chain-name [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [ttl-security hops hop-count]
no area area-id virtual-link router-id authentication key-chain chain-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area-id</td>
<td>Area ID assigned to the virtual link. This can be either a decimal value or a valid IPv6 prefix. There is no default.</td>
</tr>
<tr>
<td>router-id</td>
<td>Router ID associated with the virtual link neighbor. The router ID appears in the <code>show ip ospf</code> or <code>show ipv6 display</code> command. There is no default.</td>
</tr>
<tr>
<td>authentication</td>
<td>Enables virtual link authentication.</td>
</tr>
<tr>
<td>key-chain</td>
<td>Configures a key-chain for cryptographic authentication keys.</td>
</tr>
<tr>
<td>chain-name</td>
<td>Name of the authentication key that is valid.</td>
</tr>
<tr>
<td>hello-interval seconds</td>
<td>(Optional) Specifies the time (in seconds) between the hello packets that the Cisco IOS software sends on an interface. The hello interval is an unsigned integer value to be advertised in the hello packets. The value must be the same for all routers and access servers attached to a common network. The range is from 1 to 8192. The default is 10.</td>
</tr>
<tr>
<td>retransmit-interval seconds</td>
<td>(Optional) Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The retransmit interval is the expected round-trip delay between any two routers on the attached network. The value must be greater than the expected round-trip delay. The range is from 1 to 8192. The default is 5.</td>
</tr>
<tr>
<td>transmit-delay seconds</td>
<td>(Optional) Specifies the estimated time (in seconds) required to send a link-state update packet on the interface. The integer value that must be greater than zero. LSAs in the update packet have their age incremented by this amount before transmission. The range is from 1 to 8192. The default value is 1.</td>
</tr>
</tbody>
</table>
**dead-interval seconds**  
(Optional) Specifies the time (in seconds) that hello packets are not seen before a neighbor declares the router down. The dead interval is an unsigned integer value. The default is four times the hello interval, or 40 seconds. As with the hello interval, this value must be the same for all routers and access servers attached to a common network.

**ttl-security hops hop-count**  
(Optional) Configures Time-to-Live (TTL) security on a virtual link. The *hop-count* argument range is from 1 to 254.

### Command Default
No OSPF virtual link is defined.

### Command Modes
- Router address family topology configuration (config-router-af-topology)
- Router configuration (config-router)
- Address family configuration (config-router-af)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
In OSPF, all areas must be connected to a backbone area. A lost connection to the backbone can be repaired by establishing a virtual link.

The shorter the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. The setting of the retransmit interval should be conservative, or needless retransmissions will result. The value should be larger for serial lines and virtual links.

You should choose a transmit delay value that considers the transmission and propagation delays for the interface.

To configure a virtual link in OSPF for IPv6, you must use a router ID instead of an address. In OSPF for IPv6, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Use the *ttl-security hops* *hop-count* keywords and argument to enable checking of TTL values on OSPF packets from neighbors or to set TTL values sent to neighbors. This feature adds an extra layer of protection to OSPF.

---

**Note**
In order for a virtual link to be properly configured, each virtual link neighbor must include the transit area ID and the corresponding virtual link neighbor router ID. To display the router ID, use the *show ip ospf* or the *show ipv6 ospf* command in privileged EXEC mode.

**Note**
To remove the specified area from the software configuration, use the *no area area-id* command (with no other keywords). That is, the *no area area-id* command removes all area options, such as *area default-cost*, *area nssa*, *area range*, *area stub*, and *area virtual-link*. 
Release 12.2(33)SRB

If you plan to configure the Multitopology Routing (MTR) feature, you need to enter the `area virtual-link` command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

**Examples**

The following example establishes a virtual link with default values for all optional parameters:

```plaintext
ipv6 router ospf 1
log-adjacency-changes
area 1 virtual-link 192.168.255.1
```

The following example establishes a virtual link in OSPF for IPv6:

```plaintext
ipv6 router ospf 1
log-adjacency-changes
area 1 virtual-link 192.168.255.1 hello-interval 5
```

The following example shows how to configure TTL security for a virtual link in OSPFv3 for IPv6:

```plaintext
Device(config)#!router ospfv3 1
Device(config-router)#address-family ipv6 unicast vrf vrf1
Device(config-router-af)#area 1 virtual-link 10.1.1.1 ttl-security hops 10
```

The following example shows how to configure the authentication using a key chain for virtual-links:

```plaintext
area 1 virtual-link 1.1.1.1 authentication key-chain ospf-chain-1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area</td>
<td>Configures OSPFv3 area parameters.</td>
</tr>
<tr>
<td>show ip ospf</td>
<td>Enables the display of general information about OSPF routing processes.</td>
</tr>
<tr>
<td>show ipv6 ospf</td>
<td>Enables the display of general information about OSPF routing processes.</td>
</tr>
<tr>
<td>ttl-security hops</td>
<td>Enables checking of TTL values on OSPF packets from neighbors or setting TTL values sent to neighbors.</td>
</tr>
</tbody>
</table>
auto-summary (BGP)

To configure automatic summarization of subnet routes into network-level routes, use the `auto-summary` command in address family or router configuration mode. To disable automatic summarization and send subprefix routing information across classful network boundaries, use the `no` form of this command.

```
auto-summary
no auto-summary
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Automatic summarization is disabled by default (the software sends subprefix routing information across classful network boundaries).

**Command Modes**

Address family configuration (config-router-af)

Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

BGP automatically summarizes routes to classful network boundaries when this command is enabled. Route summarization is used to reduce the amount of routing information in routing tables. Automatic summarization applies to connected, static, and redistributed routes.

**Note**

The MPLS VPN Per VRF Label feature does not support auto-summary.

By default, automatic summarization is disabled and BGP accepts subnets redistributed from an Interior Gateway Protocol (IGP). To block subnets and create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the `auto-summary` command.

To advertise and carry subnet routes in BGP when automatic summarization is enabled, use an explicit `network` command to advertise the subnet. The `auto-summary` command does not apply to routes injected into BGP via the `network` command or through iBGP or eBGP.

**Why auto-summary for BGP Is Disabled By Default**

When `auto-summary` is enabled, routes injected into BGP via redistribution are summarized on a classful boundary. Remember that a 32-bit IP address consists of a network address and a host address. The subnet mask determines the number of bits used for the network address and the number of bits used for the host address. The IP address classes have a natural or standard subnet mask, as shown in the table below.

**Table 106: IP Address Classes**

<table>
<thead>
<tr>
<th>Class</th>
<th>Address Range</th>
<th>Standard Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>1.0.0.0 to 126.0.0.0</td>
<td>255.0.0.0 or /8</td>
</tr>
<tr>
<td>B</td>
<td>128.1.0.0 to 191.254.0.0</td>
<td>255.255.0.0 or /16</td>
</tr>
</tbody>
</table>
Reserved addresses include 128.0.0.0, 191.255.0.0, 192.0.0.0, and 223.255.255.0.

When using the standard subnet mask, Class A addresses have one octet for the network, Class B addresses have two octets for the network, and Class C addresses have three octets for the network.

Consider the Class B address 156.26.32.1 with a 24-bit subnet mask, for example. The 24-bit subnet mask selects three octets, 156.26.32, for the network. The last octet is the host address. If the network 156.26.32.1/24 is learned via an IGP and is then redistributed into BGP, if `auto-summary` were enabled, the network would be automatically summarized to the natural mask for a Class B network. The network that BGP would advertise is 156.26.0.0/16. BGP would be advertising that it can reach the entire Class B address space from 156.26.0.0 to 156.255.255.255. If the only network that can be reached via the BGP router is 156.26.32.0/24, BGP would be advertising 254 networks that cannot be reached via this router. This is why the `auto-summary` (BGP) command is disabled by default.

Examples

In the following example, automatic summarization is enabled for IPv4 address family prefixes:

```
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4 unicast
Device(config-router-af)#auto-summary
Device(config-router-af)#network 7.7.7.7 255.255.255.255
```

In the example, there are different subnets, such as 7.7.7.6 and 7.7.7.7 on Loopback interface 6 and Loopback interface 7, respectively. Both `auto-summary` and a `network` command are configured.

```
Device#show ip interface brief
Interface  IP-Address OK? Method Status Protocol
Ethernet0/0   100.0.1.7   YES NVRAM up     up
Ethernet0/1   unassigned   YES NVRAM administratively down down
Ethernet0/2   unassigned   YES NVRAM administratively down down
Ethernet0/3   unassigned   YES NVRAM administratively down down
Ethernet1/0   108.7.9.7   YES NVRAM up     up
Ethernet1/1   unassigned   YES NVRAM administratively down down
Ethernet1/2   unassigned   YES NVRAM administratively down down
Ethernet1/3   unassigned   YES NVRAM administratively down down
Loopback6    7.7.7.6     YES NVRAM up     up
Loopback7    7.7.7.7     YES NVRAM up     up
```

Note that in the output below, because of the `auto-summary` command, the BGP routing table displays the summarized route 7.0.0.0 instead of 7.7.7.6. The 7.7.7.7/32 network is displayed because it was configured with the `network` command, which is not affected by the `auto-summary` command.

```
Device#show ip bgp
BGP table version is 10, local router ID is 7.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network         Next Hop     Metric  LocPrf  Weight  Path
*> 6.6.6.6/32    100.0.1.6    0       0       6  i
*> 7.0.0.0       0.0.0.0     0       32768  ?  <-- summarization
*> 7.7.7.7/32    0.0.0.0     0       32768  i  <-- network command
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 (BGP)</td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.</td>
</tr>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>Specifies the networks to be advertised by BGP and multiprotocol BGP.</td>
</tr>
</tbody>
</table>
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**
- `authentication-type` Authentication type. Valid values are md5, meticulous-md5, meticulous-sha1, and sha-1.
- `keychain keychain-name` 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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**

- `interval milliseconds` 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 milliseconds` 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 multiplier-value` 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 it is configured is removed.
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
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.

When echo mode is enabled, the desired minimum echo transmit interval and required minimum transmit interval values are taken from the `bfd interval milliseconds min_rx milliseconds` parameters, respectively.

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
• 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.
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  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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
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 single-hop  template-name
no bfd-template single-hop  template-name
```

**Syntax Description**
- `single-hop` Creates the single-hop BFD template.
- `template-name` Template name.

**Command Default**
A BFD template does not exist.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 100 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 configured explicitly.
To enable the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors, use the `bgp graceful-restart` command in address family or in router configuration mode. To disable the BGP graceful restart capability globally for all BGP neighbors, use the `no` form of this command.

```
bgp graceful-restart [ { extended | restart-time seconds | stalepath-time seconds } ] [ all ]

no bgp graceful-restart
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extended</td>
<td>(Optional) Enables BGP graceful restart extension.</td>
</tr>
<tr>
<td>restart-time</td>
<td>(Optional) Sets the maximum time period that the local router will wait for</td>
</tr>
<tr>
<td>seconds</td>
<td>a graceful-restart-capable neighbor to return to normal operation after a</td>
</tr>
<tr>
<td></td>
<td>restart event occurs. The default value for this argument is 120 seconds.</td>
</tr>
<tr>
<td></td>
<td>The configurable range of values is from 1 to 3600 seconds.</td>
</tr>
<tr>
<td>stalepath-time</td>
<td>(Optional) Sets the maximum time period that the local router will hold</td>
</tr>
<tr>
<td>seconds</td>
<td>stale paths for a restarting peer. All stale paths are deleted after this</td>
</tr>
<tr>
<td></td>
<td>timer expires. The default value for this argument is 360 seconds. The</td>
</tr>
<tr>
<td></td>
<td>configurable range of values is from 1 to 3600 seconds.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Enables BGP graceful restart capability for all address family</td>
</tr>
<tr>
<td></td>
<td>modes.</td>
</tr>
</tbody>
</table>

### Command Default

The following default values are used when this command is entered without any keywords or arguments:

- `restart-time` : 120 seconds
- `stalepath-time`: 360 seconds

### Note

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

### Command Modes

- Address-family configuration (config-router-af)
- Router configuration (config-router)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `bgp graceful-restart` command is used to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart
capability is enabled after a BGP session has been established, the session will need to be restarted with a hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

The BGP graceful restart capability is enabled by default when a supporting version of Cisco IOS software is installed. The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Examples

In the following example, the BGP graceful restart capability is enabled:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart
```

In the following example, the restart timer is set to 130 seconds:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart restart-time 130
```

In the following example, the stalepath timer is set to 350 seconds:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart stalepath-time 350
```

In the following example, the extended keyword is used:

```
Device#configure terminal
Device(config)#router bgp 65000
Device(config-router)#bgp graceful-restart extended
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Displays information about the TCP and BGP connections to neighbors.</td>
</tr>
</tbody>
</table>
clear proximity ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear proximity ip bgp** command in privileged EXEC mode.

```
clear proximity ip bgp [ * | all | autonomous-system-number neighbor-address | peer-group group-name ] [ [ in | prefix-filter ] | out | slow | soft [ [ in | prefix-filter ] | out | slow ] ]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>(Optional) Specifies that all current BGP sessions will be reset.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Specifies the reset of all address family sessions.</td>
</tr>
<tr>
<td>autonomous-system-number</td>
<td>Number of the autonomous system in which all BGP peer sessions will be reset. Number in the range from 1 to 65535.</td>
</tr>
<tr>
<td>neighbor-address</td>
<td>Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>peer-group group-name</td>
<td>Specifies that only the identified BGP peer group will be reset.</td>
</tr>
<tr>
<td>in</td>
<td>(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.</td>
</tr>
<tr>
<td>prefix-filter</td>
<td>(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.</td>
</tr>
<tr>
<td>out</td>
<td>(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.</td>
</tr>
<tr>
<td>slow</td>
<td>(Optional) Clears slow-peer status forcefully and moves it to original update group.</td>
</tr>
<tr>
<td>soft</td>
<td>(Optional) Initiates a soft reset. Does not tear down the session.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `clear proximity ip bgp` command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Due to the complexity of some of the keywords available for the `clear proximity ip bgp` command, some of the keywords are documented as separate commands. All of the complex keywords that are documented separately start with `clear ip bgp`. For example, for information on resetting BGP connections using hard or soft reconfiguration for all BGP neighbors in IPv4 address family sessions, refer to the `clear ip bgp ipv4` command.

**Generating Updates from Stored Information**

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the `neighbor soft-reconfiguration inbound` command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

**Dynamic Inbound Soft Reset**

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the `show ip bgp neighbors` command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```
If all BGP routers support the route refresh capability, use the `clear proximity ip bgp` command with the `in` keyword. You need not use the `soft` keyword, because soft reset is automatically assumed when the route refresh capability is supported.

**Note**

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

**Examples**

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
Device# clear proximity ip bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers and a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
Device# clear proximity ip bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
Device# clear proximity ip bgp 35700
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Device# clear proximity ip bgp 65538
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Device# clear proximity ip bgp 1.2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bgp slow-peer split-update-group</code> dynamic permanent</td>
<td>Moves a dynamically detected slow peer to a slow update group.</td>
</tr>
<tr>
<td><code>clear ip bgp ipv4</code></td>
<td>Resets BGP connections using hard or soft reconfiguration for IPv4 address family sessions.</td>
</tr>
<tr>
<td><code>clear ip bgp ipv6</code></td>
<td>Resets BGP connections using hard or soft reconfiguration for IPv6 address family sessions.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>clear ip bgp vpnv4</td>
<td>Resets BGP connections using hard or soft reconfiguration for VPNv4 address family sessions.</td>
</tr>
<tr>
<td>clear ip bgp vpnv6</td>
<td>Resets BGP connections using hard or soft reconfiguration for VPNv6 address family sessions.</td>
</tr>
<tr>
<td>neighbor slow-peer split-update-group</td>
<td>Moves a dynamically detected slow peer to a slow update group.</td>
</tr>
<tr>
<td>dynamic permanent</td>
<td></td>
</tr>
<tr>
<td>neighbor soft-reconfiguration</td>
<td>Configures the Cisco IOS software to start storing updates.</td>
</tr>
<tr>
<td>router bgp</td>
<td>Configures the BGP routing process.</td>
</tr>
<tr>
<td>show ip bgp</td>
<td>Displays entries in the BGP routing table.</td>
</tr>
<tr>
<td>show ip bgp neighbors</td>
<td>Displays information about BGP and TCP connections to neighbors.</td>
</tr>
<tr>
<td>slow-peer split-update-group dynamic</td>
<td>Moves a dynamically detected slow peer to a slow update group.</td>
</tr>
<tr>
<td>permanent</td>
<td></td>
</tr>
</tbody>
</table>
default-information originate (OSPF)

To generate a default external route into an Open Shortest Path First (OSPF) routing domain, use the `default-information originate` command in router configuration or router address family topology configuration mode. To disable this feature, use the `no` form of this command.

```
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]

no default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

**Syntax Description**

- **always** (Optional) Always advertises the default route regardless of whether the software has a default route.

  **Note** The `always` keyword includes the following exception when the route map is used. When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table and the `always` keyword is ignored.

- **metric metric-value** (Optional) Metric used for generating the default route. If you omit a value and do not specify a value using the `default-metric` router configuration command, the default metric value is 10. The value used is specific to the protocol.

- **metric-type type-value** (Optional) External link type associated with the default route that is advertised into the OSPF routing domain. It can be one of the following values:
  - Type 1 external route.
  - Type 2 external route.

  The default is type 2 external route.

- **route-map map-name** (Optional) The routing process will generate the default route if the route map is satisfied.

**Command Default**

This command is disabled by default. No default external route is generated into the OSPF routing domain.

**Command Modes**

Router configuration (config-router) Router address family topology configuration (config-router-af-topology)

**Command History**

Cisco IOS XE Everest 16.5.1a This command was introduced.

**Usage Guidelines**

Whenever you use the `redistribute` or the `default-information` router configuration command to redistribute routes into an OSPF routing domain, the Cisco IOS software automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the OSPF routing domain. The software must still have a default route for itself before it generates one, except when you have specified the `always` keyword.

When a route map is used, the origination of the default route by OSPF is not bound to the existence of a default route in the routing table.
Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the `default-information originate` command in router address family topology configuration mode in order for this OSPF router configuration command to become topology-aware.

Examples

The following example specifies a metric of 100 for the default route that is redistributed into the OSPF routing domain and specifies an external metric type of 1:

```
router ospf 109
redistribute eigrp 108 metric 100 subnets
default-information originate metric 100 metric-type 1
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default-information</td>
<td>Accepts exterior or default information into Enhanced Interior Gateway Routing Protocol (EIGRP) processes.</td>
</tr>
<tr>
<td>default-metric</td>
<td>Sets default metric values for routes.</td>
</tr>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
**default-metric (BGP)**

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the `default-metric` command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the `no` form of this command.

```
default-metric number
no default-metric number
```

**Syntax Description**

| number | Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295. |

**Command Default**

The following is default behavior if this command is not configured or if the `no` form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

**Command Modes**

- Address family configuration (config-router-af)
- Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `default-metric` command is used to set the metric value for routes redistributed into BGP and can be applied to any external BGP (eBGP) routes received and subsequently advertised internally to iBGP peers. This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.

**Note**

When enabled, the `default-metric` command applies a metric value of 0 to redistributed connected routes. The `default-metric` command does not override metric values that are applied with the `redistribute` command.

**Examples**

In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```
Device(config)#router bgp 50000
Device(config-router)#address-family ipv4 unicast
Device(config-router-af)#default-metric 1024
```
In the following configuration and output examples, a metric of 300 is set for eBGP routes received and advertised internally to an iBGP peer.

After the above configuration, some routes are received from the eBGP peer at 192.168.2.2 as shown in the output from the `show ip bgp neighbors` command.

After the received routes from the eBGP peer at 192.168.2.2 are advertised internally to iBGP peers, the output from the `show ip bgp neighbors` command shows that the metric (MED) has been set to 300 for these routes.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redistribute (IP)</td>
<td>Redistributes routes from one routing domain into another routing domain.</td>
</tr>
</tbody>
</table>
To define an administrative distance, use the `distance` command in router configuration mode or VRF configuration mode. To remove the `distance` command and restore the system to its default condition, use the `no` form of this command.

```
distance  weight
  [ip-address wildcard-mask  [access-list name]]
no distance  weight ip-address wildcard-mask  [access-list-name]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>weight</code></td>
<td>Administrative distance. Range is 10 to 255. Used alone, the <code>weight</code> argument specifies a default administrative distance that the software uses when no other specification exists for a routing information source. Routes with a distance of 255 are not installed in the routing table. The table in the “Usage Guidelines” section lists the default administrative distances.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>(Optional) IP address in four-part dotted-decimal notation.</td>
</tr>
<tr>
<td><code>wildcard-mask</code></td>
<td>(Optional) Wildcard mask in four-part, dotted-decimal format. A bit set to 1 in the <code>wildcard-mask</code> argument instructs the software to ignore the corresponding bit in the address value.</td>
</tr>
<tr>
<td><code>access-list-name</code></td>
<td>(Optional) Name of an IP access list to be applied to incoming routing updates.</td>
</tr>
</tbody>
</table>

### Command Default

If this command is not specified, the administrative distance is the default. The table in the “Usage Guidelines” section lists the default administrative distances.

### Command Modes

- Router configuration (config-router)
- VRF configuration (config-vrf)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the appropriate task IDs. If the user group assignment is preventing you from using a command contact your AAA administrator for assistance.

An administrative distance is an integer from 10 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means that the routing information source cannot be trusted at all and should be ignored. Weight values are subjective; no quantitative method exists for choosing weight values.

If an access list is used with this command, it is applied when a network is being inserted into the routing table. This behavior allows you to filter networks based on the IP prefix supplying the routing information. For example, you could filter possibly incorrect routing information from networking devices not under your administrative control.

The order in which you enter `distance` commands can affect the assigned administrative distances, as shown in the “Examples” section. The following table lists default administrative distances.
### Table 110: Default Administrative Distances

<table>
<thead>
<tr>
<th>Rate Source</th>
<th>Default Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route out on interface</td>
<td>0</td>
</tr>
<tr>
<td>Static route to next hop</td>
<td>1</td>
</tr>
<tr>
<td>EIGRP summary route</td>
<td>5</td>
</tr>
<tr>
<td>External BGP</td>
<td>20</td>
</tr>
<tr>
<td>Internal EIGRP</td>
<td>90</td>
</tr>
<tr>
<td>OSPF</td>
<td>110</td>
</tr>
<tr>
<td>IS-IS</td>
<td>115</td>
</tr>
<tr>
<td>RIP version 1 and 2</td>
<td>120</td>
</tr>
<tr>
<td>External EIGRP</td>
<td>170</td>
</tr>
<tr>
<td>Internal BGP</td>
<td>200</td>
</tr>
<tr>
<td>Unknown</td>
<td>255</td>
</tr>
</tbody>
</table>

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospf</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

In the following example, the `router ospf` command sets up Open Shortest Path First (OSPF) routing instance 1. The first `distance` command sets the default administrative distance to 255, which instructs the software to ignore all routing updates from networking devices for which an explicit distance has not been set. The second `distance` command sets the administrative distance for all devices on the network 192.168.40.0 to 90.

```
Device#configure terminal
Device(config)#router ospf 1
Device(config ospf)#distance 255
Device(config ospf)#distance 90 192.168.40.0 0.0.0.255
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>distance bgp</code></td>
<td>Allows the use of external, internal, and local administrative distances that could be a better route to a BGP node.</td>
</tr>
<tr>
<td><code>distance ospf</code></td>
<td>Allows the use of external, internal, and local administrative distances that could be a better route to an OSPF node.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>router ospf</td>
<td>Configures the OSPF routing process.</td>
</tr>
</tbody>
</table>
eigrp log-neighbor-changes

To enable the logging of changes in Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, use the `eigrp log-neighbor-changes` command in router configuration mode, address-family configuration mode, or service-family configuration mode. To disable the logging of changes in EIGRP neighbor adjacencies, use the `no` form of this command.

```
eigrp log-neighbor-changes
no eigrp log-neighbor-changes
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Adjacency changes are logged.

**Command Modes**

Router configuration (config-router) Address-family configuration (config-router-af) Service-family configuration (config-router-sf)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems. Logging is enabled by default. To disable the logging of neighbor adjacency changes, use the `no` form of this command.

To enable the logging of changes for EIGRP address-family neighbor adjacencies, use the `eigrp log-neighbor-changes` command in address-family configuration mode.

To enable the logging of changes for EIGRP service-family neighbor adjacencies, use the `eigrp log-neighbor-changes` command in service-family configuration mode.

**Examples**

The following configuration disables logging of neighbor changes for EIGRP process 209:

```
Device(config)# router eigrp 209
Device(config-router)# no eigrp log-neighbor-changes
```

The following configuration enables logging of neighbor changes for EIGRP process 209:

```
Device(config)# router eigrp 209
Device(config-router)# eigrp log-neighbor-changes
```

The following example shows how to disable logging of neighbor changes for EIGRP address-family with autonomous-system 4453:

```
Device(config)# router eigrp virtual-name
Device(config-router)# address-family ipv4 autonomous-system 4453
Device(config-router-af)# no eigrp log-neighbor-changes
Device(config-router-af)# exit-address-family
```

The following configuration enables logging of neighbor changes for EIGRP service-family process 209:
Device(config)\# router eigrp 209
Device(config-router)# service-family ipv4 autonomous-system 4453
Device(config-router-sf)# eigrp log-neighbor-changes
Device(config-router-sf)# exit-service-family

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family (EIGRP)</td>
<td>Enters address-family configuration mode to configure an EIGRP routing instance.</td>
</tr>
<tr>
<td>exit-address-family</td>
<td>Exits address-family configuration mode.</td>
</tr>
<tr>
<td>exit-service-family</td>
<td>Exits service-family configuration mode.</td>
</tr>
<tr>
<td>router eigrp</td>
<td>Configures the EIGRP routing process.</td>
</tr>
<tr>
<td>service-family</td>
<td>Specifies service-family configuration mode.</td>
</tr>
</tbody>
</table>
ip authentication key-chain eigrp

To enable authentication of Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the `ip authentication key-chain eigrp` command in interface configuration mode. To disable such authentication, use the `no` form of this command.

```
ip authentication key-chain eigrp as-number key-chain
no ip authentication key-chain eigrp as-number key-chain
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>Autonomous system number to which the authentication applies.</td>
</tr>
<tr>
<td><code>key-chain</code></td>
<td>Name of the authentication key chain.</td>
</tr>
</tbody>
</table>

### Command Default

No authentication is provided for EIGRP packets.

### Command Modes

Interface configuration (config-if) Virtual network interface (config-if-vnet)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example applies authentication to autonomous system 2 and identifies a key chain named SPORTS:

```
Device(config-if)#ip authentication key-chain eigrp 2 SPORTS
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-lifetime</td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td>ip authentication mode eigrp</td>
<td>Specifies the type of authentication used in EIGRP packets.</td>
</tr>
<tr>
<td>key</td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td>key chain</td>
<td>Enables authentication of routing protocols.</td>
</tr>
<tr>
<td>key-string (authentication)</td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td>send-lifetime</td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
ip authentication mode eigrp

To specify the type of authentication used in Enhanced Interior Gateway Routing Protocol (EIGRP) packets, use the `ip authentication mode eigrp` command in interface configuration mode. To disable that type of authentication, use the `no` form of this command.

```
ip authentication mode eigrp as-number md5
no ip authentication mode eigrp as-number md5
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>as-number</code></td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td><code>md5</code></td>
<td>Keyed Message Digest 5 (MD5) authentication.</td>
</tr>
</tbody>
</table>

**Command Default**

No authentication is provided for EIGRP packets.

**Command Modes**

Interface configuration (config-if) Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Configure authentication to prevent unapproved sources from introducing unauthorized or false routing messages. When authentication is configured, an MD5 keyed digest is added to each EIGRP packet in the specified autonomous system.

**Examples**

The following example configures the interface to use MD5 authentication in EIGRP packets in autonomous system 10:

```
Device(config-if)#ip authentication mode eigrp 10 md5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accept-lifetime</code></td>
<td>Sets the time period during which the authentication key on a key chain is received as valid.</td>
</tr>
<tr>
<td><code>ip authentication key-chain eigrp</code></td>
<td>Enables authentication of EIGRP packets.</td>
</tr>
<tr>
<td><code>key</code></td>
<td>Identifies an authentication key on a key chain.</td>
</tr>
<tr>
<td><code>key chain</code></td>
<td>Enables authentication of routing protocols.</td>
</tr>
<tr>
<td><code>key-string (authentication)</code></td>
<td>Specifies the authentication string for a key.</td>
</tr>
<tr>
<td><code>send-lifetime</code></td>
<td>Sets the time period during which an authentication key on a key chain is valid to be sent.</td>
</tr>
</tbody>
</table>
**ip bandwidth-percent eigrp**

To configure the percentage of bandwidth that may be used by Enhanced Interior Gateway Routing Protocol (EIGRP) on an interface, use the `ip bandwidth-percent eigrp` command in interface configuration mode. To restore the default value, use the `no` form of this command.

```
ip bandwidth-percent eigrp as-number percent
no ip bandwidth-percent eigrp as-number percent
```

**Syntax Description**

- **as-number**: Autonomous system number.
- **percent**: Percent of bandwidth that EIGRP may use.

**Command Default**

EIGRP may use 50 percent of available bandwidth.

**Command Modes**

Interface configuration (config-if) Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

EIGRP will use up to 50 percent of the bandwidth of a link, as defined by the `bandwidth` interface configuration command. This command may be used if some other fraction of the bandwidth is desired. Note that values greater than 100 percent may be configured. The configuration option may be useful if the bandwidth is set artificially low for other reasons.

**Examples**

The following example allows EIGRP to use up to 75 percent (42 kbps) of a 56-kbps serial link in autonomous system 209:

```
Device(config)#interface serial 0
Device(config-if)#bandwidth 56
Device(config-if)#ip bandwidth-percent eigrp 209 75
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (interface)</td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
</tbody>
</table>
ip cef load-sharing algorithm

To select a Cisco Express Forwarding load-balancing algorithm, use the `ip cef load-sharing algorithm` command in global configuration mode. To return to the default universal load-balancing algorithm, use the `no` form of this command.

```
ip cef load-sharing algorithm original | universal [id]]
no ip cef load-sharing algorithm
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>original</td>
<td>Sets the load-balancing algorithm to the original algorithm based on a source and destination hash.</td>
</tr>
<tr>
<td>universal</td>
<td>Sets the load-balancing algorithm to the universal algorithm that uses a source and destination and an ID hash.</td>
</tr>
<tr>
<td>id</td>
<td>(Optional) Fixed identifier.</td>
</tr>
</tbody>
</table>

### Command Default

The universal load-balancing algorithm is selected by default. If you do not configure the fixed identifier for a load-balancing algorithm, the router automatically generates a unique ID.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The original Cisco Express Forwarding load-balancing algorithm produced distortions in load sharing across multiple devices because of the use of the same algorithm on every device. When the load-balancing algorithm is set to universal mode, each device on the network can make a different load sharing decision for each source-destination address pair, and that resolves load-balancing distortions.

### Examples

The following example shows how to enable the Cisco Express Forwarding original load-balancing algorithm:

```
Device> enable
Device# configure terminal
Device(config)# ip cef load-sharing algorithm original
Device(config)# exit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip load-sharing</td>
<td>Enables load balancing for Cisco Express Forwarding.</td>
</tr>
</tbody>
</table>
To configure a BGP community list and to control which routes are permitted or denied based on their community values, use the **ip community-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

**Standard Community Lists**

```
ip community-list {standard | standard list-name} {deny | permit} [community-number] [AA:NN]
internet [local-as] [no-advertise] [no-export] [gshut]
no ip community-list {standard | standard list-name}
```

**Expanded Community Lists**

```
ip community-list {expanded | expanded list-name} {deny | permit} regexp
no ip community-list {expanded | expanded list-name}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>standard</code></td>
<td>Standard community list number from 1 to 99 to identify one or more permit or deny groups of communities.</td>
</tr>
<tr>
<td><code>standard list-name</code></td>
<td>Configures a named standard community list.</td>
</tr>
<tr>
<td><code>deny</code></td>
<td>Denies routes that match the specified community or communities.</td>
</tr>
<tr>
<td><code>permit</code></td>
<td>Permits routes that match the specified community or communities.</td>
</tr>
<tr>
<td><code>community-number</code></td>
<td>(Optional) 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.</td>
</tr>
</tbody>
</table>
### ip community-list

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AA :NN</strong></td>
<td>(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered for each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.</td>
</tr>
<tr>
<td><strong>internet</strong></td>
<td>(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).</td>
</tr>
<tr>
<td><strong>local-as</strong></td>
<td>(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation.</td>
</tr>
<tr>
<td><strong>no-advertise</strong></td>
<td>(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).</td>
</tr>
<tr>
<td><strong>no-export</strong></td>
<td>(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.</td>
</tr>
</tbody>
</table>
### ip community-list

**gshut**  
(Optional) Specifies the Graceful Shutdown (GSHUT) community.

**expanded**  
Expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.

**expanded list-name**  
Configures a named expanded community list.

**regexp**  
Regular expression that is used to specify a pattern to match against an input string.  

**Note**  
Regular expressions can be used only with expanded community lists.

| Command Default | BGP community exchange is not enabled by default. |
| Command Modes | Global configuration (config) |
| Command History |  
**Table 111:**  

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  
The `ip community-list` command is used to filter BGP routes based on one or more community values. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the `ip bgp-community new-format` command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported.

BGP community exchange is not enabled by default. The exchange of BGP community attributes between BGP peers is enabled on a per-neighbor basis with the `neighbor send-community` command. The BGP community attribute is defined in RFC 1997 and RFC 1998.

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the `set community` command.

Use a route map to reference a community list and thereby apply policy routing or set values.

**Community List Processing**
Once a permit value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values. Unlike an access list, it is feasible for a community list to contain only deny statements.

- When multiple communities are configured in the same ip community-list statement, a logical AND condition is created. All community values for a route must match the communities in the community list statement to satisfy an AND condition.

- When multiple communities are configured in separate ip community-list statements, a logical OR condition is created. The first list that matches a condition is processed.

**Standard Community Lists**

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

**Expanded Community Lists**

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the “Regular Expressions” appendix of the Terminal Services Configuration Guide.

**Examples**

In the following example, a standard community list is configured that permits routes from network 10 in autonomous system 50000:

```
Device(config)#ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Device(config)#ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Device(config)#ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named, standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Device(config)#ip community-list standard RED permit local-as
Device(config)#ip community-list standard RED permit 40000:20
```

In the following example, a standard community list is configured that denies routes with the GSHUT community and permits routes with the local-AS community. This example shows a logical OR condition; the first match is processed.
Device(config)#ip community-list 18 deny gshut
Device(config)#ip community-list 18 permit local-as

In the following example, an expanded community list is configured that denies routes that carry communities from any private autonomous system:

Device(config)#ip community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_

In the following example, a named expanded community list is configured that denies routes from network 1 to 99 in autonomous system 50000:

Device(config)#ip community-list expanded BLUE deny 50000:[0-9][0-9]_

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>match community</td>
<td>Defines a BGP community that must match the community of a route.</td>
</tr>
<tr>
<td>neighbor send-community</td>
<td>Allows BGP community exchange with a neighbor.</td>
</tr>
<tr>
<td>neighbor shutdown graceful</td>
<td>Configures the BGP Graceful Shutdown feature.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set community</td>
<td>Sets the BGP communities attribute.</td>
</tr>
<tr>
<td>set comm-list delete</td>
<td>Removes communities from the community attribute of an inbound or outbound update.</td>
</tr>
<tr>
<td>show ip bgp community</td>
<td>Displays routes that belong to specified BGP communities.</td>
</tr>
<tr>
<td>show ip bgp regexp</td>
<td>Displays routes that match a locally configured regular expression.</td>
</tr>
</tbody>
</table>
**ip prefix-list**

To create a prefix list or to add a prefix-list entry, use the `ip prefix-list` command in global configuration mode. To delete a prefix-list entry, use the `no` form of this command.

```
ip prefix-list {list-name [seq number] [deny | permit] network/length [ge ge-length] [le le-length] | description description | sequence-number}  
no ip prefix-list {list-name [seq number] [(deny | permit) network/length [ge ge-length] [le le-length]] | description description | sequence-number}  
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list-name</td>
<td>Configures a name to identify the prefix list. Do not use the word “detail” or “summary” as a list name because they are keywords in the <code>show ip prefix-list</code> command.</td>
</tr>
<tr>
<td>seq</td>
<td>(Optional) Applies a sequence number to a prefix-list entry.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies access for a matching condition.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits access for a matching condition.</td>
</tr>
<tr>
<td>network / length</td>
<td>Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.</td>
</tr>
<tr>
<td>ge</td>
<td>(Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the <code>ge-length</code> argument to the range specified.</td>
</tr>
<tr>
<td>ge-length</td>
<td>(Optional) Represents the minimum prefix length to be matched.</td>
</tr>
<tr>
<td>le</td>
<td>(Optional) Specifies the greater value of a range (the “to” portion of the range description) by applying the <code>le-length</code> argument to the range specified.</td>
</tr>
<tr>
<td>le-length</td>
<td>(Optional) Represents the maximum prefix length to be matched.</td>
</tr>
<tr>
<td>description</td>
<td>(Optional) Configures a descriptive name for the prefix list.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>(Optional) Enables or disables the use of sequence numbers for prefix lists.</td>
</tr>
</tbody>
</table>

**Command Default**

No prefix lists or prefix-list entries are created.

**Command Modes**

Global configuration (config)
**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `ip prefix-list` command to configure IP prefix filtering. Prefix lists are configured with `permit` or `deny` keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the `ge` and `le` keywords are used. The `ge` and `le` keywords are used to specify a range of prefix lengths and provide more flexible configuration than using only the `network/length` argument. A prefix list is processed using an exact match when neither the `ge` nor `le` keyword is specified. If only the `ge` value is specified, the range is the value entered for the `ge ge-length` argument to a full 32-bit length. If only the `le` value is specified, the range is from the value entered for the `network/length` argument to the `le le-length` argument. If both the `ge ge-length` and `le le-length` keywords and arguments are entered, the range is between the values used for the `ge-length` and `le-length` arguments.

The following formula shows this behavior:

\[
\text{length} < \text{ge ge-length} \leq \text{le le-length} \leq 32
\]

If the `seq` keyword is configured without a sequence number, the default sequence number is 5. In this scenario, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5. For example, the next two entries would have sequence numbers 10 and 15. If a sequence number is entered for the first prefix list entry but not for subsequent entries, the subsequent entry numbers increment by 5. For example, if the first configured sequence number is 3, subsequent entries will be 8, 13, and 18. Default sequence numbers can be suppressed by entering the `no ip prefix-list` command with the `seq` keyword.

Evaluation of a prefix list starts with the lowest sequence number and continues down the list until a match is found. When an IP address match is found, the permit or deny statement is applied to that network and the remainder of the list is not evaluated.

**Tip**

For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The `seq number` keyword and argument can be used for resequencing.

A prefix list is applied to inbound or outbound updates for a specific peer by entering the `neighbor prefix-list` command. Prefix list information and counters are displayed in the output of the `show ip prefix-list` command. Prefix-list counters can be reset by entering the `clear ip prefix-list` command.

**Examples**

In the following example, a prefix list is configured to deny the default route 0.0.0.0/0:

```
Device(config) #ip prefix-list RED deny 0.0.0.0/0
```

In the following example, a prefix list is configured to permit traffic from the 172.16.1.0/24 subnet:

```
Device(config) #ip prefix-list BLUE permit 172.16.1.0/24
```
In the following example, a prefix list is configured to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

Device(config)#ip prefix-list YELLOW permit 10.0.0.0/8 le 24

In the following example, a prefix list is configured to deny routes from the 10.0.0.0/8 network that have a mask length that is greater than or equal to 25 bits:

Device(config)#ip prefix-list PINK deny 10.0.0.0/8 ge 25

In the following example, a prefix list is configured to permit routes from any network that have a mask length from 8 to 24 bits:

Device(config)#ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24

In the following example, a prefix list is configured to deny any route with any mask length from the 10.0.0.0/8 network:

Device(config)#ip prefix-list ORANGE deny 10.0.0.0/8 le 32

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip prefix-list</td>
<td>Resets the prefix list entry counters.</td>
</tr>
<tr>
<td>ip prefix-list description</td>
<td>Adds a text description of a prefix list.</td>
</tr>
<tr>
<td>ip prefix-list sequence</td>
<td>Enables or disables default prefix-list sequencing.</td>
</tr>
<tr>
<td>match ip address</td>
<td>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.</td>
</tr>
<tr>
<td>neighbor prefix-list</td>
<td>Filters routes from the specified neighbor using a prefix list.</td>
</tr>
<tr>
<td>show ip prefix-list</td>
<td>Displays information about a prefix list or prefix list entries.</td>
</tr>
</tbody>
</table>
**ip hello-interval eigrp**

To configure the hello interval for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the `ip hello-interval eigrp` command in interface configuration mode. To restore the default value, use the `no` form of this command.

```
ip hello-interval eigrp as-number seconds
no ip hello-interval eigrp as-number [seconds]
```

**Syntax Description**

| as-number | Autonomous system number. |
| seconds   | Hello interval (in seconds). The range is from 1 to 65535. |

**Command Default**

The hello interval for low-speed, nonbroadcast multiaccess (NBMA) networks is 60 seconds and 5 seconds for all other networks.

**Command Modes**

Interface configuration (config-if) Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The default of 60 seconds applies only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the `bandwidth` interface configuration command. Note that for the purposes of EIGRP, Frame Relay and Switched Multimegabit Data Service (SMDS) networks may be considered to be NBMA. These networks are considered NBMA if the interface has not been configured to use physical multicasting; otherwise, they are considered not to be NBMA.

**Examples**

The following example sets the hello interval for Ethernet interface 0 to 10 seconds:

```
Device(config)#interface ethernet 0
Device(config-if)#ip hello-interval eigrp 10 10
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth (interface)</td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
<tr>
<td>ip hold-time eigrp</td>
<td>Configures the hold time for a particular EIGRP routing process designated by the autonomous system number.</td>
</tr>
</tbody>
</table>
ip hold-time eigrp

To configure the hold time for an Enhanced Interior Gateway Routing Protocol (EIGRP) process, use the \texttt{ip hold-time eigrp} command in interface configuration mode. To restore the default value, use the \texttt{no} form of this command.

\texttt{ip hold-time eigrp as-number seconds}

\no ip hold-time eigrp as-number seconds

\begin{tabular}{|l|l|}
\hline
\textbf{Syntax Description} & \\
\hline
as-number & Autonomous system number. \\
seconds & Hold time (in seconds). The range is from 1 to 65535. \\
\hline
\end{tabular}

\textbf{Command Default}

The EIGRP hold time is 180 seconds for low-speed, nonbroadcast multiaccess (NBMA) networks and 15 seconds for all other networks.

\textbf{Command Modes}

Interface configuration (config-if) Virtual network interface (config-if-vnet)

\textbf{Command History}

\begin{tabular}{|l|l|}
\hline
\textbf{Release} & \textbf{Modification} \\
\hline
Cisco IOS XE Everest 16.5.1a & This command was introduced. \\
\hline
\end{tabular}

\textbf{Usage Guidelines}

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If a router does not receive a hello packet within the specified hold time, routes through this router are considered unavailable.

Increasing the hold time delays route convergence across the network.

The default of 180 seconds hold time and 60 seconds hello interval apply only to low-speed, NBMA media. Low speed is considered to be a rate of T1 or slower, as specified with the \texttt{bandwidth} interface configuration command.

\textbf{Examples}

The following example sets the hold time for Ethernet interface 0 to 40 seconds:

\begin{verbatim}
Device(config)#interface ethernet 0
Device(config-if)#ip hold-time eigrp 109 40
\end{verbatim}

\textbf{Related Commands}

\begin{tabular}{|l|l|}
\hline
\textbf{Command} & \textbf{Description} \\
\hline
\texttt{bandwidth (interface)} & Sets a bandwidth value for an interface. \\
\texttt{ip hello-interval eigrp} & Configures the hello interval for the EIGRP routing process designated by an autonomous system number. \\
\hline
\end{tabular}
To enable load balancing for Cisco Express Forwarding on an interface, use the `ip load-sharing` command in interface configuration mode. To disable load balancing for Cisco Express Forwarding on the interface, use the `no` form of this command.

```
ip load-sharing {per-packet | per-destination}
oip load-sharing per-packet
```

### Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>per-packet</strong></td>
<td>Enables per-packet load balancing for Cisco Express Forwarding on the interface. This functionality and keyword are not supported on all platforms. See &quot;Usage Guidelines&quot; for more information.</td>
</tr>
<tr>
<td><strong>per-destination</strong></td>
<td>Enables per-destination load balancing for Cisco Express Forwarding on the interface.</td>
</tr>
</tbody>
</table>

### Command Default

Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Per-packet load balancing allows the router to send data packets over successive equal-cost paths without regard to individual destination hosts or user sessions. Path utilization is good, but packets destined for a given destination host might take different paths and might arrive out of order.

Per-destination load balancing allows the device to use multiple, equal-cost paths to achieve load sharing. Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple, equal-cost paths are available. Traffic for different source-destination host pairs tends to take different paths.

**Note**

If you want to enable per-packet load sharing to a particular destination, then all interfaces that can forward traffic to the destination must be enabled for per-packet load sharing.

### Examples

The following example shows how to enable per-packet load balancing:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip load-sharing per-packet
```

The following example shows how to enable per-destination load balancing:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ip load-sharing per-destination
```
ip next-hop-self eigrp

To enable the Enhanced Interior Gateway Routing Protocol (EIGRP) to advertise routes with the local outbound interface address as the next hop, use the `ip next-hop-self eigrp` command in interface configuration mode or virtual network interface mode. To instruct EIGRP to use the received next hop instead of the local outbound interface address, use the `no` form of this command.

```
ip next-hop-self eigrp as-number
no ip next-hop-self eigrp as-number
```

**Syntax Description**

- `as-number`: Autonomous system number.

**Command Default**

The IP next-hop-self state is enabled.

**Command Modes**

Interface configuration (config-if)

Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

EIGRP, by default, sets the next-hop value to the local outbound interface address for routes that it is advertising, even when advertising those routes back out of the same interface on which they were learned. To change this default, you must use the `no ip next-hop-self eigrp` interface configuration command to instruct EIGRP to use the received next-hop value when advertising these routes. Following are some exceptions to this guideline:

- If your topology does not require spoke-to-spoke dynamic tunnels, you need not configure the `no ip next-hop-self eigrp` command.
- If your topology requires spoke-to-spoke dynamic tunnels, you must use process switching on the tunnel interface of spoke devices. Otherwise, you will need to use a different routing protocol over Dynamic Multipoint VPN (DMVPN).

**Examples**

The following example shows how to change the default next-hop value in IPv4 classic mode configurations by disabling the `ip next-hop-self` functionality and configuring EIGRP to use the received next-hop value to advertise routes:

```
Device(config)#interface tun 0
Device(config-if)#no ip next-hop-self eigrp 101
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 next-hop self eigrp</code></td>
<td>Instructs an EIGRP device that the IPv6 next hop is the local outbound interface.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>next-hop-self</td>
<td>Enables EIGRP to advertise routes with the local outbound interface address as the next hop.</td>
</tr>
</tbody>
</table>
ip ospf database-filter all out

To filter outgoing link-state advertisements (LSAs) to an Open Shortest Path First (OSPF) interface, use the `ip ospf database-filter all out` command in interface or virtual network interface configuration modes. To restore the forwarding of LSAs to the interface, use the `no` form of this command.

```
ip ospf database-filter all out [disable]
no ip ospf database-filter all out
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>disable</code></td>
<td>(Optional) Disables the filtering of outgoing LSAs to an OSPF interface; all outgoing LSAs are flooded to the interface.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This keyword is available only in virtual network interface mode.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled by default. All outgoing LSAs are flooded to the interface.

**Command Modes**

- Interface configuration (config-if)
- Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command performs the same function that the `neighbor database-filter` command performs on a neighbor basis.

If the `ip ospf database-filter all out` command is enabled for a virtual network and you want to disable it, use the `disable` keyword in virtual network interface configuration mode.

**Examples**

The following example prevents filtering of OSPF LSAs to broadcast, nonbroadcast, or point-to-point networks reachable through Ethernet interface 0:

```
Device(config)#interface ethernet 0
Device(config-if)#ip ospf database-filter all out
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>neighbor database-filter</strong></td>
<td>Filters outgoing LSAs to an OSPF neighbor.</td>
<td></td>
</tr>
</tbody>
</table>
ip ospf name-lookup

To configure Open Shortest Path First (OSPF) to look up Domain Name System (DNS) names for use in all OSPF show EXEC command displays, use the ip ospf name-lookup command in global configuration mode. To disable this function, use the no form of this command.

`ip ospf name-lookup`
`noipospfname-lookup`

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

**Command Default**
This command is disabled by default.

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command makes it easier to identify a router because the router is displayed by name rather than by its router ID or neighbor ID.

**Examples**
The following example configures OSPF to look up DNS names for use in all OSPF show EXEC command displays:

```
Device(config)#ip ospf name-lookup
```
ip split-horizon eigrp

To enable Enhanced Interior Gateway Routing Protocol (EIGRP) split horizon, use the ip split-horizon eigrp command in interface configuration mode. To disable split horizon, use the no form of this command.

```
ip split-horizon eigrp as-number
no ip split-horizon eigrp as-number
```

**Syntax Description**

| as-number | Autonomous system number |

**Command Default**

The behavior of this command is enabled by default.

**Command Modes**

- Interface configuration (config-if)
- Virtual network interface (config-if-vnet)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the no ip split-horizon eigrp command to disable EIGRP split horizon in your configuration.

**Examples**

The following is an example of how to enable EIGRP split horizon:

```
Device(config-if)#ip split-horizon eigrp 101
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip split-horizon (RIP)</td>
<td>Enables the split horizon mechanism.</td>
</tr>
<tr>
<td>neighbor (EIGRP)</td>
<td>Defines a neighboring router with which to exchange routing information.</td>
</tr>
</tbody>
</table>
ip summary-address eigrp

To configure address summarization for the Enhanced Interior Gateway Routing Protocol (EIGRP) on a specified interface, use the **ip summary-address eigrp** command in interface configuration or virtual network interface configuration mode. To disable the configuration, use the **no** form of this command.

```
ip summary-address eigrp as-number ip-address mask [admin-distance] [leak-map name]
no ip summary-address eigrp as-number ip-address mask
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-number</td>
<td>Autonomous system number.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Summary IP address to apply to an interface.</td>
</tr>
<tr>
<td>mask</td>
<td>Subnet mask.</td>
</tr>
<tr>
<td>admin-distance</td>
<td>(Optional) Administrative distance. Range: 0 to 255.</td>
</tr>
</tbody>
</table>

**Note** Starting with Cisco IOS XE Release 3.2S, the `admin-distance` argument was removed. Use the `summary-metric` command to configure the administrative distance.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>leak-map name</td>
<td>(Optional) Specifies the route-map reference that is used to configure the route leaking through the summary.</td>
</tr>
</tbody>
</table>

### Command Default

- An administrative distance of 5 is applied to EIGRP summary routes.
- EIGRP automatically summarizes to the network level, even for a single host route.
- No summary addresses are predefined.
- The default administrative distance metric for EIGRP is 90.

### Command Modes

Interface configuration (config-if)

Virtual network interface configuration (config-if-vnet)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **ip summary-address eigrp** command is used to configure interface-level address summarization. EIGRP summary routes are given an administrative-distance value of 5. The administrative-distance metric is used to advertise a summary without installing it in the routing table.

By default, EIGRP summarizes subnet routes to the network level. The **no auto-summary** command can be entered to configure the subnet-level summarization.

The summary address is not advertised to the peer if the administrative distance is configured as 255.

**EIGRP Support for Leaking Routes**
Configuring the `leak-map` keyword allows a component route that would otherwise be suppressed by the manual summary to be advertised. Any component subset of the summary can be leaked. A route map and access list must be defined to source the leaked route.

The following is the default behavior if an incomplete configuration is entered:

- If the `leak-map` keyword is configured to reference a nonexistent route map, the configuration of this keyword has no effect. The summary address is advertised but all component routes are suppressed.

- If the `leak-map` keyword is configured but the access list does not exist or the route map does not reference the access list, the summary address and all component routes are advertised.

If you are configuring a virtual-network trunk interface and you configure the `ip summary-address eigrp` command, the `admin-distance` value of the command is not inherited by the virtual networks running on the trunk interface because the administrative distance option is not supported in the `ip summary-address eigrp` command on virtual network subinterfaces.

### Examples

The following example shows how to configure an administrative distance of 95 on Ethernet interface 0/0 for the 192.168.0.0/16 summary address:

```
Device(config)#router eigrp 1
Device(config-router)#no auto-summary
Device(config-router)#exit
Device(config)#interface Ethernet 0/0
Device(config-if)#ip summary-address eigrp 1 192.168.0.0 255.255.0.0 95
```

The following example shows how to configure the 10.1.1.0/24 subnet to be leaked through the 10.2.2.0 summary address:

```
Device(config)#router eigrp 1
Device(config-router)#exit
Device(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Device(config)#route-map LEAK-10-1-1 permit 10
Device(config-route-map)#match ip address 1
Device(config-route-map)#exit
Device(config)#interface Serial 0/0
Device(config-if)#ip summary-address eigrp 1 10.2.2.0 255.0.0.0 leak-map LEAK-10-1-1
Device(config-if)#end
```

The following example configures GigabitEthernet interface 0/0/0 as a virtual network trunk interface:

```
Device(config)#interface gigabitethernet 0/0/0
Device(config-if)#vnet global
Device(config-if-vnet)#ip summary-address eigrp 1 10.3.3.0 255.0.0.0 33
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>auto-summary (EIGRP)</strong></td>
<td>Configures automatic summarization of subnet routes to network-level routes (default behavior).</td>
</tr>
<tr>
<td>summary-metric</td>
<td>Configures fixed metrics for an EIGRP summary aggregate address.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface-type interface-number</code></td>
<td>Interface type and number.</td>
</tr>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the gateway, in A.B.C.D format.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>Specifies Virtual Routing and Forwarding (VRF) instance and the destination vrf name.</td>
</tr>
<tr>
<td><code>group group-name</code></td>
<td>(Optional) Assigns a BFD group. The group-name is a character string of up to 32 characters specifying the BFD group name.</td>
</tr>
<tr>
<td><code>unassociate</code></td>
<td>(Optional) Unassociates the static route configured for a BFD.</td>
</tr>
</tbody>
</table>

**Command Default**

No static route BFD neighbors are specified.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.
   
   \[ \text{bfd interval milliseconds min_rx milliseconds multiplier multiplier-value} \]

2. Enable BFD for the static IP route
   
   \[ \text{ip route static bfd interface-type interface-number ip-address} \]

3. Disable and enable the BFD timers on the SVI again.
   
   \[ \text{no bfd interval milliseconds min_rx milliseconds multiplier multiplier-value} \]

   \[ \text{bfd interval milliseconds min_rx milliseconds multiplier multiplier-value} \]

### Examples

The following example shows how to configure BFD for all static routes through a specified neighbor, group, and active member of the group:

```bash
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:

```bash
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:

```bash
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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Name of the virtual routing and forwarding (VRF) instance by which static routes should be specified.</td>
</tr>
<tr>
<td>interface-type interface-number</td>
<td>Interface type and number.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>IPv6 address of the neighbor.</td>
</tr>
<tr>
<td>unassociated</td>
<td>(Optional) Moves a static BFD neighbor from associated mode to unassociated mode.</td>
</tr>
</tbody>
</table>

**Command Default**

No static route BFDv6 neighbors are specified.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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(config)terminal
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1
```

The following example converts the neighbor to unassociated mode:

```
Device(config)#ipv6 route static bfd ethernet 0/0 2001::1 unassociated
```
**metric weights (EIGRP)**

To tune the Enhanced Interior Gateway Routing Protocol (EIGRP) metric calculations, use the `metric weights` command in router configuration mode or address family configuration mode. To reset the values to their defaults, use the `no` form of this command.

**Router Configuration**

```
metric weights tos k1 k2 k3 k4 k5
```

```
no metric weights
```

**Address Family Configuration**

```
metric weights [tos k1 [k2 [k3 [k4 [k5 [k6]]]]]]
```

```
no metric weights
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>tos</th>
<th>Type of service. This value must always be zero.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>k1</td>
<td>(Optional) Constants that convert an EIGRP metric vector into a scalar quantity. Valid values are 0 to 255. Given below are the default values:</td>
</tr>
<tr>
<td></td>
<td>k2</td>
<td>• k1: 1</td>
</tr>
<tr>
<td></td>
<td>k3</td>
<td>• k2: 0</td>
</tr>
<tr>
<td></td>
<td>k4</td>
<td>• k3: 1</td>
</tr>
<tr>
<td></td>
<td>k5</td>
<td>• k4: 0</td>
</tr>
<tr>
<td></td>
<td>k6</td>
<td>• k5: 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• k6: 0</td>
</tr>
</tbody>
</table>

**Command Default**

EIGRP metric K values are set to their default values.

**Command Modes**

- Router configuration (config-router)
- Address family configuration (config-router-af)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to alter the default behavior of EIGRP routing and metric computation and to allow the tuning of the EIGRP metric calculation for a particular type of service (ToS).

If k5 equals 0, the composite EIGRP metric is computed according to the following formula:

\[
\text{metric} = [k1 \times \text{bandwidth} + (k2 \times \text{bandwidth})/(256 - \text{load}) + k3 \times \text{delay} + K6 \times \text{extended metrics}]
\]
If \( k5 \) does not equal zero, an additional operation is performed:

\[
\text{metric} = \frac{\text{metric} \times k5}{\text{reliability} + k4}
\]

Scaled Bandwidth = \( 10^7 / \text{minimum interface bandwidth (in kilobits per second)} \times 256 \)

Delay is in tens of microseconds for classic mode and picoseconds for named mode. In classic mode, a delay of hexadecimal FFFFFFFFF (decimal 4294967295) indicates that the network is unreachable. In named mode, a delay of hexadecimal FFFFFFFF (decimal 281474976710655) indicates that the network is unreachable.

Reliability is given as a fraction of 255. That is, 255 is 100 percent reliability or a perfectly stable link.

Load is given as a fraction of 255. A load of 255 indicates a completely saturated link.

**Examples**

The following example shows how to set the metric weights to slightly different values than the defaults:

```
Device(config)#router eigrp 109
Device(config-router)#network 192.168.0.0
Device(config-router)#metric weights 0 2 0 2 0 0
```

The following example shows how to configure an address-family metric weight to ToS: 0; K1: 2; K2: 0; K3: 2; K4: 0; K5: 0; K6: 1:

```
Device(config)#router eigrp virtual-name
Device(config-router)#address-family ipv4 autonomous-system 4533
Device(config-router-af)#metric weights 0 2 0 2 0 0 1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address-family (EIGRP)</code></td>
<td>Enters address family configuration mode to configure an EIGRP routing instance.</td>
</tr>
<tr>
<td><code>bandwidth (interface)</code></td>
<td>Sets a bandwidth value for an interface.</td>
</tr>
<tr>
<td><code>delay (interface)</code></td>
<td>Sets a delay value for an interface.</td>
</tr>
<tr>
<td><code>ipv6 router eigrp</code></td>
<td>Configures an IPv6 EIGRP routing process.</td>
</tr>
<tr>
<td><code>metric holddown</code></td>
<td>Keeps new EIGRP routing information from being used for a certain period of time.</td>
</tr>
<tr>
<td><code>metric maximum-hops</code></td>
<td>Causes IP routing software to advertise routes with a hop count higher than what is specified by the command (EIGRP only) as unreachable routes.</td>
</tr>
<tr>
<td><code>router eigrp</code></td>
<td>Configures an EIGRP routing process.</td>
</tr>
</tbody>
</table>
To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the `neighbor advertisement-interval` command in address family or router configuration mode. To restore the default value, use the `no` form of this command.

```
neighbor {ip-address peer-group-name} advertisement-interval seconds
no neighbor {ip-address peer-group-name} advertisement-interval seconds
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>seconds</td>
<td>Time (in seconds) is specified by an integer ranging from 0 to 600.</td>
</tr>
</tbody>
</table>

**Command Default**

- eBGP sessions not in a VRF: 30 seconds
- eBGP sessions in a VRF: 0 seconds
- iBGP sessions: 0 seconds

**Command Modes**

Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes. If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

**Examples**

The following router configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
neighbor 10.4.4.4 advertisement-interval 10
```

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
address-family ipv4 unicast
neighbor 10.4.4.4 advertisement-interval 10
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4 (BGP)</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family vpnv4</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPLS address prefixes.</td>
</tr>
<tr>
<td><strong>neighbor peer-group (creating)</strong></td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the `neighbor default-originate` command in address family or router configuration mode. To send no route as a default, use the `no` form of this command.

```
neighbor {ip-address peer-group-name} default-originate [route-map map-name]
no neighbor {ip-address peer-group-name} default-originate [route-map map-name]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>route-map</td>
<td></td>
<td>(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.</td>
</tr>
</tbody>
</table>

Command Default

No default route is sent to the neighbor.

Command Modes

- Address family configuration (config-router-af)
- Router configuration (config-router)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a `match ip address` clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

You can use standard or extended access lists with the `neighbor default-originate` command.

Examples

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
network 172.16.0.0
neighbor 172.16.2.3 remote-as 200
neighbor 172.16.2.3 default-originate route-map default-map
```
route-map default-map 10 permit
   match ip address 1
!
access-list 1 permit 192.168.68.0

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 with a mask of 255.255.0.0:

router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
   match ip address 100
!
access-list 100 permit ip host 192.168.68.0 host 255.255.0.0

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 (BGP)</td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.</td>
</tr>
<tr>
<td>neighbor ebgp-multihop</td>
<td>Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.</td>
</tr>
</tbody>
</table>
neighbor description

To associate a description with a neighbor, use the `neighbor description` command in router configuration mode or address family configuration mode. To remove the description, use the `no` form of this command.

```
neighbor {ip-address peer-group-name} description text
no neighbor {ip-address peer-group-name} description [text]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of an EIGRP peer group. This argument is not available in address-family configuration mode.</td>
</tr>
<tr>
<td><code>text</code></td>
<td>Text (up to 80 characters in length) that describes the neighbor.</td>
</tr>
</tbody>
</table>

**Command Default**

There is no description of the neighbor.

**Command Modes**

Router configuration (config-router) Address family configuration (config-router-af)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

In the following examples, the description of the neighbor is “peer with example.com”:

```
Device(config)#router bgp 109
Device(config-router)#network 172.16.0.0
Device(config-router)#neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the address family neighbor is “address-family-peer”:

```
Device(config)#router eigrp virtual-name
Device(config-router)#address-family ipv4 autonomous-system 4453
Device(config-router-af)#network 172.16.0.0
Device(config-router-af)#neighbor 172.16.2.3 description address-family-peer
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family (EIGRP)</td>
<td>Enters address family configuration mode to configure an EIGRP routing instance.</td>
</tr>
<tr>
<td>network (EIGRP)</td>
<td>Specifies the network for an EIGRP routing process.</td>
</tr>
<tr>
<td>router eigrp</td>
<td>Configures the EIGRP address family process.</td>
</tr>
</tbody>
</table>
neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the `neighbor ebgp-multihop` command in router configuration mode. To return to the default, use the `no` form of this command.

```
neighbor {ip-address ipv6-address peer-group-name} ebgp-multihop [ttl]
no neighbor {ip-address ipv6-address peer-group-name} ebgp-multihop
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>IPv6 address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td><code>ttl</code></td>
<td>(Optional) Time-to-live in the range from 1 to 255 hops.</td>
</tr>
</tbody>
</table>

### Command Default

Only directly connected neighbors are allowed.

### Command Modes

Router configuration (config-router)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

### Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
Device(config)#router bgp 109
Device(config-router)#neighbor 10.108.1.1 ebgp-multihop
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>neighbor advertise-map non-exist-map</code></td>
<td>Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.</td>
</tr>
<tr>
<td><code>neighbor peer-group (creating)</code></td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td><code>network (BGP and multiprotocol BGP)</code></td>
<td>Specifies the list of networks for the BGP routing process.</td>
</tr>
</tbody>
</table>
neighbor maximum-prefix (BGP)

To control how many prefixes can be received from a neighbor, use the `neighbor maximum-prefix` command in router configuration mode. To disable this function, use the `no` form of this command.

```
neighbor {ip-address peer-group-name} maximum-prefix maximum [threshold] [restart restart-interval] [warning-only]
no neighbor {ip-address peer-group-name} maximum-prefix maximum
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>peer-group-name</td>
<td>Name of a Border Gateway Protocol (BGP) peer group.</td>
</tr>
<tr>
<td>maximum</td>
<td>Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.</td>
</tr>
<tr>
<td>threshold</td>
<td>(Optional) Integer specifying at what percentage of the maximum-prefix limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.</td>
</tr>
<tr>
<td>restart</td>
<td>(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The restart timer is configured with the <code>restart-interval</code> argument.</td>
</tr>
<tr>
<td>restart-interval</td>
<td>(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.</td>
</tr>
<tr>
<td>warning-only</td>
<td>(optional) Allows the router to generate a sys-log message when the maximum-prefix limit is exceeded, instead of terminating the peering session.</td>
</tr>
</tbody>
</table>

### Command Default

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If the `restart-interval` argument is not configured, a disabled session will stay down after the maximum-prefix limit is exceeded.

`threshold`: 75 percent

### Command Modes

Router configuration (config-router)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `neighbor maximum-prefix` command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process will accept from the specified peer. This feature provides a mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If the `restart` keyword is configured, BGP will automatically reestablish the peering session.
session at the configured time interval. If the restart keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceeded, the peering session will not be reestablished until the clear ip bgp command is entered. If the warning-only keyword is configured, BGP sends only a log message and continues to peer with the sender.

There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources.

Examples

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.1.1 maximum-prefix 1000
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.2.2 maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

In the following example, warning messages will be displayed when the threshold of the maximum-prefix limit (500 x 0.75 = 375) for the 192.168.4.4 neighbor is exceeded:

```
Device(config)#router bgp 40000
Device(config-router)#network 192.168.0.0
Device(config-router)#neighbor 192.168.4.4 maximum-prefix 500 warning-only
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear ip bgp</td>
<td>Resets a BGP connection using BGP soft reconfiguration.</td>
</tr>
</tbody>
</table>
neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the `neighbor peer-group` command in address family or router configuration mode. To remove the neighbor from the peer group, use the `no` form of this command.

```
neighbor {ip-address|ipv6-address} peer-group peer-group-name
no neighbor {ip-address|ipv6-address} peer-group peer-group-name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the BGP neighbor that belongs to the peer group specified by the <code>peer-group-name</code> argument.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>IPv6 address of the BGP neighbor that belongs to the peer group specified by the <code>peer-group-name</code> argument.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of the BGP peer group to which this neighbor belongs.</td>
</tr>
</tbody>
</table>

**Command Default**

There are no BGP neighbors in a peer group.

**Command Modes**

- Address family configuration (config-router-af)
- Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The neighbor at the IP address indicated inherits all the configured options of the peer group.

**Note**

Using the `no` form of the `neighbor peer-group` command removes all of the BGP configuration for that neighbor, not just the peer group association.

**Examples**

The following router configuration mode example assigns three neighbors to the peer group named `internal`:

```
Device(config)#router bgp 100
Device(config-router)#neighbor internal peer-group
Device(config-router)#neighbor internal remote-as 100
Device(config-router)#neighbor internal update-source loopback 0
Device(config-router)#neighbor internal route-map set-med out
Device(config-router)#neighbor internal filter-list 1 out
Device(config-router)#neighbor internal filter-list 2 in
Device(config-router)#neighbor 172.16.232.53 peer-group internal
Device(config-router)#neighbor 172.16.232.54 peer-group internal
```
Device(config-router)#neighbor 172.16.232.55 peer-group internal
Device(config-router)#neighbor 172.16.232.55 filter-list 3 in

The following address family configuration mode example assigns three neighbors to the peer group named internal:

Device(config)#router bgp 100
Device(config-router)#address-family ipv4 unicast
Device(config-router)#neighbor internal peer-group
Device(config-router)#neighbor internal remote-as 100
Device(config-router)#neighbor internal update-source loopback 0
Device(config-router)#neighbor internal route-map set-med out
Device(config-router)#neighbor internal filter-list 1 out
Device(config-router)#neighbor internal filter-list 2 in
Device(config-router)#neighbor 172.16.232.53 peer-group internal
Device(config-router)#neighbor 172.16.232.54 peer-group internal
Device(config-router)#neighbor 172.16.232.55 peer-group internal
Device(config-router)#neighbor 172.16.232.55 filter-list 3 in

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv4 (BGP)</td>
<td>Places the router in address family configuration mode for configuring</td>
</tr>
<tr>
<td></td>
<td>routing sessions such as BGP, RIP, or static routing sessions that use</td>
</tr>
<tr>
<td></td>
<td>standard IPv4 address prefixes.</td>
</tr>
<tr>
<td>address-family vpnv4</td>
<td>Places the router in address family configuration mode for configuring</td>
</tr>
<tr>
<td></td>
<td>routing sessions such as BGP, RIP, or static routing sessions that use</td>
</tr>
<tr>
<td></td>
<td>standard VPIv4 address prefixes.</td>
</tr>
<tr>
<td>neighbor peer-group (creating)</td>
<td>Creates a BGP peer group.</td>
</tr>
<tr>
<td>neighbor shutdown</td>
<td>Disables a neighbor or peer group.</td>
</tr>
</tbody>
</table>
neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the `neighbor peer-group` command in address family or router configuration mode. To remove the peer group and all of its members, use the `no` form of this command.

```
neighbor  peer-group-name peer-group
no neighbor  peer-group-name peer-group
```

**Syntax Description**

| peer-group-name | Name of the BGP peer group. |

**Command Default**

There is no BGP peer group.

**Command Modes**

- Address family configuration (config-router-af)
- Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

**Note**

Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the `neighbor peer-group` command, it can be configured with the `neighbor` commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the `neighbor {ip-address | peer-group-name} remote-as` command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

### Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the `router bgp` command and the `neighbor remote-as` command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The `neighbor internal filter-list 2 in` command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 172.16.232.53 peer-group internal
neighbor 172.16.232.54 peer-group internal
neighbor 172.16.232.55 peer-group internal
neighbor 172.16.232.55 filter-list 3 in
```

The following example defines the peer group named external-peers without the `neighbor remote-as` command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 172.16.232.90 remote-as 200
neighbor 172.16.232.90 peer-group external-peers
neighbor 172.16.232.100 remote-as 300
neighbor 172.16.232.100 peer-group external-peers
neighbor 172.16.232.110 remote-as 400
neighbor 172.16.232.110 peer-group external-peers
neighbor 172.16.232.110 filter-list 400 in
```

In the following example, all members of the peer group are multicast-capable:
router bgp 100
neighbor 10.1.1.1 remote-as 1
neighbor 172.16.2.2 remote-as 2
address-family ipv4 multicast
neighbor mygroup peer-group
neighbor 10.1.1.1 peer-group mygroup
neighbor 172.16.2.2 peer-group mygroup
neighbor 10.1.1.1 activate
neighbor 172.16.2.2 activate

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4 (BGP)</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family vpnv4</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.</td>
</tr>
<tr>
<td><strong>clear ip bgp peer-group</strong></td>
<td>Removes all the members of a BGP peer group.</td>
</tr>
<tr>
<td><strong>show ip bgp peer-group</strong></td>
<td>Displays information about BGP peer groups.</td>
</tr>
</tbody>
</table>
neighbor route-map

To apply a route map to incoming or outgoing routes, use the `neighbor route-map` command in address family or router configuration mode. To remove a route map, use the `no` form of this command.

```
neighbor {ip-address peer-group-name | ipv6-address{[\%]}]} route-map map-name {in | out}
no neighbor {ip-address peer-group-name | ipv6-address{[\%]}]} route-map map-name {in | out}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td><code>peer-group-name</code></td>
<td>Name of a BGP or multiprotocol BGP peer group.</td>
</tr>
<tr>
<td><code>ipv6-address</code></td>
<td>IPv6 address of the neighbor.</td>
</tr>
<tr>
<td><code>%</code></td>
<td>(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.</td>
</tr>
<tr>
<td><code>map-name</code></td>
<td>Name of a route map.</td>
</tr>
<tr>
<td><code>in</code></td>
<td>Applies route map to incoming routes.</td>
</tr>
<tr>
<td><code>out</code></td>
<td>Applies route map to outgoing routes.</td>
</tr>
</tbody>
</table>

### Command Default

No route maps are applied to a peer.

### Command Modes

Router configuration (config-router)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the `peer-group-name` argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The `%` keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

### Examples

The following router configuration mode example applies a route map named `internal-map` to a BGP incoming route from 172.16.70.24:

```
router bgp 5
```
The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
neighbor 172.16.70.24 route-map internal-map in
route-map internal-map
match as-path 1
set local-preference 100
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4 (BGP)</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family ipv6</strong></td>
<td>Enters address family configuration mode for configuring routing sessions that use standard IPv6 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family vpnv4</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family vpnv6</strong></td>
<td>Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Creates a BGP peer group.</td>
</tr>
</tbody>
</table>
neighbor update-source

To have the Cisco software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the \texttt{neighbor update-source} command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the \texttt{no} form of this command.

\texttt{neighbor\{ip-address|ipv6-address\}\{\%\}\{peer-group-name\}\update-source\ interface-type\ interface-number}

**Syntax Description**

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>\texttt{ip-address}</td>
<td>IPv4 address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td>\texttt{ipv6-address}</td>
<td>IPv6 address of the BGP-speaking neighbor.</td>
</tr>
<tr>
<td>\texttt{%}</td>
<td>(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.</td>
</tr>
<tr>
<td>\texttt{peer-group-name}</td>
<td>Name of a BGP peer group.</td>
</tr>
<tr>
<td>\texttt{interface-type}</td>
<td>Interface type.</td>
</tr>
<tr>
<td>\texttt{interface-number}</td>
<td>Interface number.</td>
</tr>
</tbody>
</table>

**Command Default**

Best local address

**Command Modes**

Router configuration (config-router)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can work in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Cisco IOS Interface and Hardware Component Configuration Guide.

If you specify a BGP peer group by using the \texttt{peer-group-name} argument, all the members of the peer group will inherit the characteristic configured with this command.

The \texttt{neighbor update-source} command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The \% keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes \texttt{<IPv6 local-link address>\%<interface name>}, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The \% keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

**Examples**

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:
Device(config)#router bgp 65000
Device(config-router)#network 172.16.0.0
Device(config-router)#neighbor 172.16.2.3 remote-as 110
Device(config-router)#neighbor 172.16.2.3 update-source Loopback0

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

Device(config)#router bgp 65000
Device(config-router)#neighbor 3ffe::3 remote-as 65000
Device(config-router)#neighbor 3ffe::3 update-source Loopback0
Device(config-router)#neighbor fe80::2%Ethernet1/0 remote-as 65400
Device(config-router)#neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
Device(config-router)#address-family ipv6
Device(config-router)#neighbor 3ffe::3 activate
Device(config-router)#neighbor fe80::2%Ethernet1/0 activate
Device(config-router)#exit-address-family

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor activate</td>
<td>Enables the exchange of information with a BGP neighboring router.</td>
</tr>
<tr>
<td>neighbor remote-as</td>
<td>Adds an entry to the BGP or multiprotocol BGP neighbor table.</td>
</tr>
</tbody>
</table>
network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the `network` command in address family or router configuration mode. To remove an entry from the routing table, use the `no` form of this command.

```
network  {network-number [mask network-mask] nsap-prefix} [route-map map-tag]
network  {network-number [mask network-mask] nsap-prefix} [route-map map-tag]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network-number</code></td>
<td>Network that BGP or multiprotocol BGP will advertise.</td>
</tr>
<tr>
<td><code>mask</code> <code>network-mask</code></td>
<td>(Optional) Network or subnetwork mask with mask address.</td>
</tr>
<tr>
<td><code>nsap-prefix</code></td>
<td>Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.</td>
</tr>
<tr>
<td><code>route-map</code> <code>map-tag</code></td>
<td>(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.</td>
</tr>
</tbody>
</table>

### Command Default

No networks are specified.

### Command Modes

- Address family configuration (config-router-af)
- Router configuration (config-router)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of `network` commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

### Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
Device(config)#router bgp 65100
Device(config-router)#network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
Device(config)#router bgp 64800
```
Device(config-router)#**address family ipv4 multicast**
Device(config-router)#**network 10.108.0.0**

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

Device(config)#**router bgp 64500**
Device(config-router)#**address-family nsap**
Device(config-router)#**network 49.6001**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>address-family ipv4</strong> (BGP)</td>
<td>Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.</td>
</tr>
<tr>
<td><strong>address-family vpnv4</strong></td>
<td>Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.</td>
</tr>
<tr>
<td><strong>default-information originate</strong> (BGP)</td>
<td>Allows the redistribution of network 0.0.0.0 into BGP.</td>
</tr>
<tr>
<td><strong>route-map (IP)</strong></td>
<td>Defines the conditions for redistributing routes from one routing protocol into another.</td>
</tr>
<tr>
<td><strong>router bgp</strong></td>
<td>Configures the BGP routing process.</td>
</tr>
</tbody>
</table>
network (EIGRP)

To specify the network for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the `network` command in router configuration mode or address-family configuration mode. To remove an entry, use the `no` form of this command.

```
network  ip-address  [wildcard-mask]
no  network  ip-address  [wildcard-mask]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the directly connected network.</td>
</tr>
<tr>
<td><code>wildcard-mask</code></td>
<td>(Optional) EIGRP wildcard bits. Wildcard mask indicates a subnet, bitwise complement of the subnet mask.</td>
</tr>
</tbody>
</table>

**Command Default**

No networks are specified.

**Command Modes**

Router configuration (config-router) Address-family configuration (config-router-af)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the `network` command is configured for an EIGRP routing process, the router matches one or more local interfaces. The `network` command matches only local interfaces that are configured with addresses that are within the same subnet as the address that has been configured with the `network` command. The router then establishes neighbors through the matched interfaces. There is no limit to the number of network statements (`network` commands) that can be configured on a router.

Use a wildcard mask as a shortcut to group networks together. A wildcard mask matches everything in the network part of an IP address with a zero. Wildcard masks target a specific host/IP address, entire network, subnet, or even a range of IP addresses.

When entered in address-family configuration mode, this command applies only to named EIGRP IPv4 configurations. Named IPv6 and Service Advertisement Framework (SAF) configurations do not support this command in address-family configuration mode.

**Examples**

The following example configures EIGRP autonomous system 1 and establishes neighbors through network 172.16.0.0 and 192.168.0.0:

```
Device(config)#router eigrp 1
Device(config-router)#network 172.16.0.0
Device(config-router)#network 192.168.0.0
Device(config-router)#network 192.168.0.0 0.0.255.255
```

The following example configures EIGRP address-family autonomous system 4453 and establishes neighbors through network 172.16.0.0 and 192.168.0.0:

```
Device(config)#router eigrp virtual-name
Device(config-router)#address-family ipv4 autonomous-system 4453
```
Device(config-router-af)#network 172.16.0.0
Device(config-router-af)#network 192.168.0.0

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>address-family (EIGRP)</td>
<td>Enters address-family configuration mode to configure an EIGRP routing instance.</td>
</tr>
<tr>
<td></td>
<td>router eigrp</td>
<td>Configures the EIGRP address-family process.</td>
</tr>
</tbody>
</table>
nsf (EIGRP)

To enable Cisco nonstop forwarding (NSF) operations for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the `nsf` command in router configuration or address family configuration mode. To disable EIGRP NSF and to remove the EIGRP NSF configuration from the running-configuration file, use the `no` form of this command.

```nsf	no nsf```

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

**Command Default**
EIGRP NSF is disabled.

**Command Modes**
- Router configuration (config-router)
- Address family configuration (config-router-af)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `nsf` command is used to enable or disable EIGRP NSF support on an NSF-capable router. NSF is supported only on platforms that support High Availability.

**Examples**
The following example shows how to disable NSF:

```Device#configure terminal
Device(config)#router eigrp 101
Device(config-router)#no nsf
Device(config-router)#end```

The following example shows how to enable EIGRP IPv6 NSF:

```Device#configure terminal
Device(config)#router eigrp virtual-name-1
Device(config-router)#address-family ipv6 autonomous-system 10
Device(config-router-af)#nsf
Device(config-router-af)#end```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug eigrp address-family ipv6 notifications</code></td>
<td>Displays information about EIGRP address family IPv6 event notifications.</td>
</tr>
<tr>
<td><code>debug eigrp nsf</code></td>
<td>Displays notifications and information about NSF events for an EIGRP routing process.</td>
</tr>
<tr>
<td><code>debug ip eigrp notifications</code></td>
<td>Displays information and notifications for an EIGRP routing process.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>show ip protocols</td>
<td>Displays the parameters and the current state of the active routing protocol process.</td>
</tr>
<tr>
<td>show ipv6 protocols</td>
<td>Displays the parameters and the current state of the active IPv6 routing protocol process.</td>
</tr>
<tr>
<td>timers graceful-restart purge-time</td>
<td>Sets the graceful-restart purge-time timer to determine how long an NSF-aware router that is running EIGRP must hold routes for an inactive peer.</td>
</tr>
<tr>
<td>timers nsf converge</td>
<td>Sets the maximum time that the restarting router must wait for the end-of-table notification from an NSF-capable or NSF-aware peer.</td>
</tr>
<tr>
<td>timers nsf signal</td>
<td>Sets the maximum time for the initial restart period.</td>
</tr>
</tbody>
</table>
offset-list (EIGRP)

To add an offset to incoming and outgoing metrics to routes learned via Enhanced Interior Gateway Routing Protocol (EIGRP), use the offset-list command in router configuration mode or address family topology configuration mode. To remove an offset list, use the no form of this command.

```
offset-list {access-list-number access-list-name} {in | out} offset [interface-type interface-number]
no offset-list {access-list-number access-list-name} {in | out} offset [interface-type interface-number]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-list-number</td>
<td>Standard access list number or name to be applied. Access list number 0 indicates all networks (networks, prefixes, or routes). If the offset value is 0, no action is taken.</td>
</tr>
<tr>
<td>access-list-name</td>
<td></td>
</tr>
<tr>
<td>in</td>
<td>Applies the access list to incoming metrics.</td>
</tr>
<tr>
<td>out</td>
<td>Applies the access list to outgoing metrics.</td>
</tr>
<tr>
<td>offset</td>
<td>Positive offset to be applied to metrics for networks matching the access list. If the offset is 0, no action is taken.</td>
</tr>
<tr>
<td>interface-type</td>
<td>(Optional) Interface type to which the offset list is applied.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Interface number to which the offset list is applied.</td>
</tr>
</tbody>
</table>

### Command Default

No offset values are added to incoming or outgoing metrics to routes learned via EIGRP.

### Command Modes

Router configuration (config-router) Address family topology configuration (config-router-af-topology)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The offset value is added to the routing metric. An offset list with an interface type and interface number is considered extended and takes precedence over an offset list that is not extended. Therefore, if an entry passes the extended offset list and the normal offset list, the offset of the extended offset list is added to the metric.

### Examples

In the following example, the router applies an offset of 10 to the delay component of the router only to access list 21:

```
Device(config-router)#offset-list 21 out 10
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0:

```
Device(config-router)#offset-list 21 in 10 ethernet 0
```

In the following example, the router applies an offset of 10 to routes learned from Ethernet interface 0 in an EIGRP named configuration:
Device(config)#router eigrp virtual-name
Device(config-router)#address-family ipv4 autonomous-system 1
Device(config-router-af)#topology base
Device(config-router-af-topology)#offset-list 21 in 10 ethernet0
router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the `router bgp` command in global configuration mode. To remove a BGP routing process, use the `no` form of this command.

```
router bgp autonomous-system-number
no router bgp autonomous-system-number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>autonomous-system-number</code></td>
<td>Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Command Default**

No BGP routing process is enabled by default.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Cisco has implemented the following two methods of representing autonomous system numbers:

- **Asplain**—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.

- **Asdot**—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see [RFC 5396](https://tools.ietf.org/html/rfc5396).

---

In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

---

**Note**

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the
default `show` command output to display 4-byte autonomous system numbers in the asdot format, use the `bgp asnotation dot` command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display `show` command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in `show` command output and to control matching for regular expressions in the asdot format, you must configure the `bgp asnotation dot` command. After enabling the `bgp asnotation dot` command, a hard reset must be initiated for all BGP sessions by entering the `clear ip bgp *` command.

If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The `show` command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

### Table 124: Default Asplain 4-Byte Autonomous System Number Format

<table>
<thead>
<tr>
<th>Format</th>
<th>Configuration Format</th>
<th>Show Command Output and Regular Expression Match Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>asplain</td>
<td>2-byte: 1 to 65535 4-byte: 65536 to 4294967295</td>
<td>2-byte: 1 to 65535 4-byte: 65536 to 4294967295</td>
</tr>
<tr>
<td>asplain</td>
<td>2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535</td>
<td>2-byte: 1 to 65535 4-byte: 65536 to 4294967295</td>
</tr>
</tbody>
</table>

### Table 125: Asdot 4-Byte Autonomous System Number Format

<table>
<thead>
<tr>
<th>Format</th>
<th>Configuration Format</th>
<th>Show Command Output and Regular Expression Match Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>asplain</td>
<td>2-byte: 1 to 65535 4-byte: 65536 to 4294967295</td>
<td>2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535</td>
</tr>
<tr>
<td>asplain</td>
<td>2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535</td>
<td>2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535</td>
</tr>
</tbody>
</table>

### Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(33)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXH, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

**RFC 5398, Autonomous System (AS) Number Reservation for Documentation Use**, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.
Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. Cisco recommends that ISPs filter private autonomous system numbers.

Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: http://www.iana.org/.

### Examples

The following example shows how to configure a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 45000
Device(config-router)# neighbor 192.168.1.2 remote-as 40000
Device(config-router)# neighbor 192.168.3.2 remote-as 50000
Device(config-router)# neighbor 192.168.3.2 description finance
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 192.168.1.2 activate
Device(config-router-af)# neighbor 192.168.3.2 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0
Device(config-router-af)# exit-address-family
```

The following example shows how to configure a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(33)S2, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65538
Device(config-router)# neighbor 192.168.1.2 remote-as 65536
Device(config-router)# neighbor 192.168.3.2 remote-as 65550
Device(config-router)# neighbor 192.168.3.2 description finance
Device(config-router)# address-family ipv4
Device(config-router-af)# neighbor 192.168.1.2 activate
Device(config-router-af)# neighbor 192.168.3.2 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# no synchronization
Device(config-router-af)# network 172.17.1.0 mask 255.255.255.0
Device(config-router-af)# exit-address-family
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor remote-as</td>
<td>Adds an entry to the BGP or multiprotocol BGP neighbor table.</td>
</tr>
<tr>
<td>network (BGP and multiprotocol BGP)</td>
<td>Specifies the list of networks for the BGP routing process.</td>
</tr>
</tbody>
</table>
router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To force Open Shortest Path First (OSPF) to use the previous OSPF router ID behavior, use the **no** form of this command.

```
router-id  ip-address
no router-id  ip-address
```

**Syntax Description**

| ip-address | Router ID in IP address format. |

**Command Default**

No OSPF routing process is defined.

**Command Modes**

Router configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique.

If this command is used on an OSPF router process which is already active (has neighbors), the new router-ID is used at the next reload or at a manual OSPF process restart. To manually restart the OSPF process, use the `clear ip ospf` command.

**Examples**

The following example specifies a fixed router-id:

```
router-id 10.1.1.1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear ip ospf</td>
<td>Clears redistribution based on the OSPF routing process ID.</td>
</tr>
<tr>
<td>router ospf</td>
<td>Configures the OSPF routing process.</td>
</tr>
</tbody>
</table>
router eigrp

To configure the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process, use the `router eigrp` command in global configuration mode. To remove an EIGRP routing process, use the `no` form of this command.

```
router eigrp {autonomous-system-number virtual-instance-name}
no router eigrp {autonomous-system-number virtual-instance-name}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>autonomous-system-number</code></td>
<td>Autonomous system number that identifies the services to the other EIGRP address-family routers. It is also used to tag routing information. Valid range is 1 to 65535.</td>
</tr>
<tr>
<td><code>virtual-instance-name</code></td>
<td>EIGRP virtual instance name. This name must be unique among all address-family router processes on a single router, but need not be unique among routers.</td>
</tr>
</tbody>
</table>

### Command Default

No EIGRP processes are configured.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Configuring the `router eigrp` command with the `autonomous-system-number` argument creates an EIGRP configuration referred to as autonomous system (AS) configuration. An EIGRP AS configuration creates an EIGRP routing instance that can be used for tagging routing information.

Configuring the `router eigrp` command with the `virtual-instance-name` argument creates an EIGRP configuration referred to as EIGRP named configuration. An EIGRP named configuration does not create an EIGRP routing instance by itself. An EIGRP named configuration is a base configuration that is required to define address-family configurations under it that are used for routing.

### Examples

The following example configures EIGRP process 109:

```
Device(config)# router eigrp 109
```

The following example configures an EIGRP address-family routing process and assigns it the name “virtual-name”:

```
Device(config)# router eigrp virtual-name
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network (EIGRP)</td>
<td>Specifies a list of networks for the EIGRP process.</td>
</tr>
</tbody>
</table>
redistribute (IPv6)

To redistribute IPv6 routes from one routing domain into another routing domain, use the redistribute command in IPv6 address family configuration mode. To disable redistribution, use the no form of this command.

```
redistribute protocol [{process-id}][{include-connected {level-1 | level-1-2 | level-2}}][{as-number}][{metric metric-value}][{metric-type type-value}][{nssa-only}][{tag tag-value}][{route-map map-tag}]
```

```
no redistribute protocol [{process-id}][{include-connected {level-1 | level-1-2 | level-2}}][{as-number}][{metric metric-value}][{metric-type type-value}][{nssa-only}][{tag tag-value}][{route-map map-tag}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>Source protocol from which routes are redistributed. It can be one of the following keywords: bgp, connected, eigrp, isis, lisp, nd, omp, ospf (ospfv3), rip, or static.</td>
<td>bgp to redistribute from bgp.</td>
</tr>
<tr>
<td>process-id</td>
<td>(Optional) For the bgp or eigrp keyword, the process ID is an autonomous system number, which is a 16-bit decimal number. For the isis keyword, the process ID is an optional value that defines a meaningful name for a routing process. You can specify only one Intermediate System-to-Intermediate System (IS-IS) process per router. Creating a name for a routing process means that you use names when configuring routing. For the ospf keyword, the process ID is the number that is assigned administratively when the Open Shortest Path First (OSPF) for the IPv6 routing process is enabled. For the rip keyword, the process ID is an optional value that defines a meaningful name for an IPv6 Routing Information Protocol (RIP) routing process.</td>
<td>process-id 100 to redistribute from ospf.</td>
</tr>
<tr>
<td>include-connected</td>
<td>(Optional) Allows the target protocol to redistribute routes that are learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running.</td>
<td>include-connected to redistribute from connected.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies that for IS-IS, Level 1 routes are redistributed into other IPv6 routing protocols independently.</td>
<td>level-1 to redistribute from level-1.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies that for IS-IS, both Level 1 and Level 2 routes are redistributed into other IPv6 routing protocols.</td>
<td>level-1-2 to redistribute from level-1-2.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies that for IS-IS, Level 2 routes are redistributed into other IPv6 routing protocols independently.</td>
<td>level-2 to redistribute from level-2.</td>
</tr>
<tr>
<td>as-number</td>
<td>(Optional) Autonomous system number for the redistributed route.</td>
<td>as-number 100 to redistribute from as-number.</td>
</tr>
<tr>
<td>metric</td>
<td>(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric is carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified.</td>
<td>metric 10 to redistribute from metric.</td>
</tr>
</tbody>
</table>
### redistribute (IPv6)

| **metric-type** | (Optional) Specifies the external link type that is associated with the default route that is advertised into the routing domain. It can be one of two values:
| **type-value** | - 1: Type 1 external route  
| | - 2: Type 2 external route  
| If no value is specified for the **metric-type** keyword, the Cisco IOS software adopts a Type 2 external route. |

| **nssa-only** | (Optional) Limits redistributed routes to not-so-stubby area (NSSA) |

| **tag** | (Optional) Specifies the 32-bit decimal value that is attached to each external route. This is not used by OSPF itself. It might be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, then the remote autonomous system number is used for routes from the BGP and the Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used. |

| **route-map** | (Optional) Specifies the route map that is checked to filter the import of routes from this source routing protocol to the current routing protocol. If the **route-map** keyword is not specified, all the routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes are imported. |

| **map-tag** | (Optional) Identifier of a configured route map. |

### Command Modes
- Router configuration (config-router)
- Address family configuration (config-router-af)

### Command History

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Changing or disabling a keyword does not affect the state of other keywords.

IS-IS ignores configured redistribution of routes, if any that are configured with the **include-connected** keyword. IS-IS advertises a prefix on an interface if either IS-IS is running over the interface or the interface is configured as passive.

Routes that are learned from IPv6 routing protocols are redistributed into IPv6 IS-IS at Level 1 into an attached area, or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

For IPv6 RIP, use the **redistribute** command to advertise static routes as if they were directly connected routes.

### Note

Advertising static routes as directly connected routes might cause routing loops if improperly configured.

Redistributed IPv6 RIP routing information is always filtered by the **distribute-list prefix-list** command in router configuration mode. Using the **distribute-list prefix-list** command ensures that only those routes that are intended by the administrator are passed along to the receiving routing protocol.
The **metric** value that is specified in the `redistribute` command for IPv6 RIP supersedes the **metric** value that is specified using the `default-metric` command.

In IPv4, if you redistribute a protocol, by default, you also redistribute the subnet on the interfaces over which the protocol is running. In IPv6, this is not the default behavior. To redistribute the subnet on the interfaces over which the protocol is running in IPv6, use the **include-connected** keyword. In IPv6, this functionality is not supported when the source protocol is BGP.

When the `no redistribute` command is configured, the parameter settings are ignored when the client protocol is IS-IS or EIGRP.

IS-IS redistribution is removed completely when IS-IS Level 1 and Level 2 are removed by you. IS-IS level settings can be configured using the `redistribute` command only.

The default redistribute type is restored to OSPFv3 when all route type values are removed by you.

Specify the **nssa-only** keyword to clear the propagate bit (P-bit) when external routes are redistributed into an NSSA. Doing so prevents corresponding NSSA external link state advertisements (LSAs) from being translated into other areas.

### Examples

The following example shows how to configure IPv6 IS-IS to redistribute IPv6 BGP routes. The metric is specified as 5, and the metric type is set to 1.

```
Device> enable
Device# configure terminal
Device(config)# router isis
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute bgp 64500 metric 5 metric-type 1
```

The following example shows how to redistribute IPv6 BGP routes into the IPv6 RIP routing process named cisco:

```
Device> enable
Device# configure terminal
Device(config)# router rip cisco
Device(config-router)# redistribute bgp 42
```

The following example shows how to redistribute IS-IS for IPv6 routes into the OSPFv3 for IPv6 routing process 1:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute isis 1 metric 32 metric-type 1 tag 85
```
**redistribute maximum-prefix (OSPF)**

To limit the number of prefixes that are redistributed into Open Shortest Path First (OSPF) or to generate a warning when the number of prefixes that are redistributed into OSPF reaches a maximum, use the `redistribute maximum-prefix` command in router configuration mode. To remove the values, use the `no` form of this command.

```
redistribute maximum-prefix maximum [{percentage}] [{warning-only}]
no redistribute
```

**Syntax Description**

- `maximum` Integer from 1 to 4294967295 that specifies the maximum number of IP or IPv6 prefixes that can be redistributed into OSPF.
  
  When the `warning-only` keyword is configured, the maximum value specifies the number of prefixes that can be redistributed into OSPF before the system logs a warning message. Redistribution is not limited.
  
  The maximum number of IP or IPv6 prefixes that are allowed to be redistributed into OSPF, or the number of prefixes that are allowed to be redistributed into OSPF before the system logs a warning message, depends on whether the `warning-only` keyword is present.
  
  There is no default value for the maximum argument.
  
  If the `warning-only` keyword is also configured, this value does not limit redistribution; it is simply the number of redistributed prefixes that, when reached, causes a warning message to be logged.

- `percentage` (Optional) Integer from 1 to 100 that specifies the threshold value, as a percentage, at which a warning message is generated.
  
  The default percentage is 75.

- `warning-only` (Optional) Causes a warning message to be logged when the number of prefixes that are defined by the `maximum` argument has been exceeded. Additional redistribution is not prevented.

**Command Default**

The default percentage is 75.

**Command Modes**

Router configuration (config-router)  
Address family configuration (config-router-af)

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

A network can be severely flooded if many IP or IPv6 prefixes are injected into the OSPF, perhaps by redistributing Border Gateway Protocol (BGP) into OSPF. Limiting the number of redistributed prefixes prevents this potential problem.

When the `redistribute maximum-prefix` command is configured and the number of redistributed prefixes reaches the maximum value that is configured, no more prefixes are redistributed (unless the `warning-only` keyword is configured).
The following example shows how two warning messages are logged; the first if the number of prefixes redistributed reaches 85 percent of 600 (510 prefixes), and the second if the number of redistributed routes reaches 600. However, the number of redistributed routes is not limited.

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 11
Device(config-router)# address-family ipv6
Device(config-router-af)# redistribute eigrp 10 subnets
Device(config-router-af)# redistribute maximum-prefix 600 85 warning-only
```

The following example shows how to set a maximum of 10 prefixes that can be redistributed into an OSPFv3 process:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 10
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# redistribute maximum-prefix 10
Device(config-router-af)# redistribute connected
```
**rewrite-evpn-rt-asn**

To enable the rewrite of the autonomous system number (ASN) portion of the EVPN route-target extended community, that originates from the current autonomous system and is advertised to an eBGP EVPN peer, with the ASN of the target eBGP EVPN peer. Use the no form of the command to disable the rewrite of ASN.

```
rewrite-evpn-rt-asn
no rewrite-evpn-rt-asn
```

**Command Modes**

Address-family configuration (config-router-af)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.12.1</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `rewrite-evpn-rt-asn` command is required for the route target auto feature to be used to configure EVPN route-targets. On Cisco Catalyst 9000 series switches, this feature is implemented on all border leaf switches that support BGP EVPN.

The `rewrite-evpn-rt-asn` command only affects the following:

- EVPN address family.
- Inbound route-reception.
- Routes from eBGP peers.
- Route-type 2 and route-type 5 of EVPN prefixes.
- Route-target extended community inside the BGP update.

The `rewrite-evpn-rt-asn` command only works on type 0 and on type 2 of route-target extended communities.

**Note**

If the Route Target auto feature is not being used, i.e., matching route targets are manually configured on all switches, then this command is not necessary.

The following example shows a configuration example of the `rewrite-evpn-rt-asn` command:

```
Device# configure terminal
Device(config)# router bgp 10000
Device(config-router)# address-family l2vpn evpn
Device(config-router-af)# rewrite-evpn-rt-asn
```
To configure an Open Shortest Path First (OSPF) routing process, use the `router ospf` command in global configuration mode. To terminate an OSPF routing process, use the `no` form of this command.

```
router ospf  process-id [vrf vrf-name]
no router ospf  process-id [vrf vrf-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>process-id</code></td>
<td>Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.</td>
</tr>
</tbody>
</table>

**Command Default**

No OSPF routing process is defined.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can specify multiple OSPF routing processes in each router.

After you enter the `router ospf` command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

**Examples**

The following example configures an OSPF routing process and assign a process number of 109:

```
Device(config)#router ospf 109
```

This example shows a basic OSPF configuration using the `router ospf` command to configure OSPF VRF instance processes for the VRFs first, second, and third:

```
Device>enable
Device#configure terminal
Device(config)#router ospf 12 vrf first
Device(config)#router ospf 13 vrf second
Device(config)#router ospf 14 vrf third
Device(config)#exit
```

The following example shows usage of the `maximum-paths` option:

```
Device>enable
Device#configure terminal
Device(config)#router ospf
Device(config)#router ospf maximum-paths?
Device(config-router)#maximum-paths 2
Device(config-router)#exit
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network area</td>
<td>Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.</td>
</tr>
</tbody>
</table>
# router ospfv3

To enter Open Shortest Path First Version 3 (OSPFv3) through router configuration mode, use the `router ospfv3` command in global configuration mode.

```
router ospfv3 [{process-id}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. The number that is used here is the number assigned administratively when enabling the OSPFv3 routing process. The range is 1-65535.</td>
</tr>
</tbody>
</table>

## Command Default

OSPFv3 routing process is disabled by default.

## Command Modes

Global configuration (config)

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Use the `router ospfv3` command to enter OSPFv3 router configuration mode. From this mode, you can enter address-family configuration mode for IPv6 or IPv4, and then configure the IPv6 or IPv4 address family.

## Examples

The following example shows how to enter OSPFv3 router configuration mode:

```
Device> enable
Device# configure terminal
Device(config)# router ospfv3 1
Device(config-router)#
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family ipv6</td>
<td>Enters IPv6 address family configuration mode.</td>
</tr>
</tbody>
</table>
set community

To set the BGP communities attribute, use the set community route map configuration command. To delete the entry, use the no form of this command.

```
set community  {community-number  [additive]  [well-known-community]  |  none}
no set community
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Community Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>community-number</td>
<td>Specifies that community number. Valid values are from 1 to 4294967200, no-export, or no-advertise.</td>
</tr>
<tr>
<td>additive</td>
<td>(Optional) Adds the community to the already existing communities.</td>
</tr>
</tbody>
</table>
| well-known-community| (Optional) Well know communities can be specified by using the following keywords:  
  - internet  
  - local-as  
  - no-advertise  
  - no-export  
| none                | (Optional) Removes the community attribute from the prefixes that pass the route map. |

**Command Default**

No BGP communities attributes exist.

**Command Modes**

Route-map configuration (config-route-map)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the route-map global configuration command, and the match and set route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria --the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions --the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.
Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

route-map set_community 10 permit
match as-path 1
set community 109
route-map set_community 20 permit
match as-path 2
set community no-export

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to peers outside the local autonomous system).

route-map set_community 10 permit
match as-path 1
set community 109
route-map set_community 20 permit
match as-path 2
set community local-as

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip community-list</td>
<td>Creates a community list for BGP and control access to it.</td>
</tr>
<tr>
<td>match community</td>
<td>Matches a BGP community.</td>
</tr>
<tr>
<td>route-map (IP)</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.</td>
</tr>
<tr>
<td>set comm-list delete</td>
<td>Removes communities from the community attribute of an inbound or outbound update.</td>
</tr>
<tr>
<td>show ip bgp community</td>
<td>Displays routes that belong to specified BGP communities.</td>
</tr>
</tbody>
</table>
set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the `set ip next-hop` command in route-map configuration mode. To delete an entry, use the `no` form of this command.

```
set ip next-hop  ip-address[...ip-address] [peer-address]
no set ip next-hop  ip-address[...ip-address] [peer-address]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>IP address of the next hop to which packets are output. It need not be an adjacent router.</td>
</tr>
<tr>
<td><strong>peer-address</strong></td>
<td>(Optional) Sets the next hop to be the BGP peering address.</td>
</tr>
</tbody>
</table>

**Command Default**

This command is disabled by default.

**Command Modes**

Route-map configuration (config-route-map)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the `ip-address` argument.

Use the `ip policy route-map` interface configuration command, the `route-map` global configuration command, and the `match` and `set` route-map configuration commands to define the conditions for policy routing packets. The `ip policy route-map` command identifies a route map by name. Each `route-map` command has a list of `match` and `set` commands associated with it. The `match` commands specify the `match criteria` -- the conditions under which policy routing occurs. The `set` commands specify the `set actions` -- the particular routing actions to perform if the criteria enforced by the `match` commands are met.

If the first next hop specified with the `set ip next-hop` command is down, the optionally specified IP addresses are tried in turn.

When the `set ip next-hop` command is used with the `peer-address` keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the `set ip next-hop` command is used with the `peer-address` keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The `set ip next-hop` command has finer granularity than the (per-neighbor) `neighbor next-hop-self` command, because you can set the next hop for some routes, but not others. The `neighbor next-hop-self` command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. `set ip next-hop`
2. `set interface`
3. `set ip default next-hop`
4. **set default interface**

To avoid a common configuration error for reflected routes, do not use the `set ip next-hop` command in a route map to be applied to BGP route reflector clients.

Configuring the `set ip next-hop ...ip-address` command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the `...ip-address` argument matches that of the specified VRF instance.

**Examples**

In the following example, three routers are on the same FDDI LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The `set ip next-hop peer-address` command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```plaintext
Device(config)#router bgp 200
Device(config)#neighbor 10.1.1.3 remote-as 300
Device(config)#neighbor 10.1.1.3 route-map set-peer-address out
Device(config)#neighbor 10.1.1.1 remote-as 100
Device(config)#route-map set-peer-address permit 10
Device(config)#set ip next-hop peer-address
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip policy route-map</code></td>
<td>Identifies a route map to use for policy routing on an interface.</td>
</tr>
<tr>
<td><code>match ip address</code></td>
<td>Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.</td>
</tr>
<tr>
<td><code>match length</code></td>
<td>Bases policy routing on the Level 3 length of a packet.</td>
</tr>
<tr>
<td><code>neighbor next-hop-self</code></td>
<td>Disables next hop processing of BGP updates on the router.</td>
</tr>
<tr>
<td><code>route-map (IP)</code></td>
<td>Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.</td>
</tr>
<tr>
<td><code>set default interface</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.</td>
</tr>
<tr>
<td><code>set interface</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing.</td>
</tr>
<tr>
<td><code>set ip default next-hop</code></td>
<td>Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.</td>
</tr>
</tbody>
</table>
show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

```
show ip bgp [ {ip-address [ {mask [ {longer-prefixes [ {injected} ] ] } | {shorter-prefixes [ {length} ] } | {best-path-reason} | {bestpath} | {multipaths} | {subnets} } ] | {best-path-reason} | {bestpath} | {internal} | {multipaths} } ] | {all} | {oer-paths} | {prefix-list name} | {pending-prefixes} | {route-map name} | {version [ {version-number} | {recent offset-value} ] } ]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.</td>
</tr>
<tr>
<td><strong>mask</strong></td>
<td>(Optional) Mask to filter or match hosts that are part of the specified network.</td>
</tr>
<tr>
<td><strong>longer-prefixes</strong></td>
<td>(Optional) Displays the specified route and all more-specific routes.</td>
</tr>
<tr>
<td><strong>injected</strong></td>
<td>(Optional) Displays more-specific prefixes injected into the BGP routing table.</td>
</tr>
<tr>
<td><strong>shorter-prefixes</strong></td>
<td>(Optional) Displays the specified route and all less-specific routes.</td>
</tr>
<tr>
<td><strong>length</strong></td>
<td>(Optional) The prefix length. The range is a number from 0 to 32.</td>
</tr>
<tr>
<td><strong>bestpath</strong></td>
<td>(Optional) Displays the best path for this prefix.</td>
</tr>
<tr>
<td><strong>best-path-reason</strong></td>
<td>(Optional) Displays the reason why a path loses to the bestpath.</td>
</tr>
<tr>
<td><strong>internal</strong></td>
<td>(Optional) Displays the internal details for this prefix.</td>
</tr>
<tr>
<td><strong>multipaths</strong></td>
<td>(Optional) Displays multipaths for this prefix.</td>
</tr>
<tr>
<td><strong>subnets</strong></td>
<td>(Optional) Displays the subnet routes for the specified prefix.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>(Optional) Displays all address family information in the BGP routing table.</td>
</tr>
<tr>
<td><strong>oer-paths</strong></td>
<td>(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.</td>
</tr>
<tr>
<td><strong>prefix-list name</strong></td>
<td>(Optional) Filters the output based on the specified prefix list.</td>
</tr>
<tr>
<td><strong>pending-prefixes</strong></td>
<td>(Optional) Displays prefixes that are pending deletion from the BGP routing table.</td>
</tr>
<tr>
<td><strong>route-map name</strong></td>
<td>(Optional) Filters the output based on the specified route map.</td>
</tr>
<tr>
<td><strong>version version-number</strong></td>
<td>(Optional) Displays all prefixes with network versions greater than or equal to the specified version number. The range is from 1 to 4294967295.</td>
</tr>
<tr>
<td><strong>recent offset-value</strong></td>
<td>(Optional) Displays the offset from the current routing table version. The range is from 1 to 4294967295.</td>
</tr>
</tbody>
</table>
show ip bgp

Command Modes

- User EXEC (>)
- Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>The <strong>best-path-reason</strong> keyword was added to this command.</td>
</tr>
<tr>
<td></td>
<td>BGP Path Installation Time-Stamp was added to the output of the command.</td>
</tr>
<tr>
<td></td>
<td>BGP Peak Prefix Watermark was added to the output of the command.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The `show ip bgp` command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

When changes are made to the network address, the network version number is incremented. Use the `version` keyword to view a specific network version.

**show ip bgp: Example**

The following sample output displays the BGP routing table:

```
Device#show ip bgp
BGP table version is 6, local router ID is 10.0.96.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>N* 10.0.0.1</td>
<td>10.0.0.3</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>?</td>
</tr>
<tr>
<td>N* 10.0.3.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>?</td>
</tr>
<tr>
<td>Nr 10.0.0.0/8</td>
<td>10.0.0.3</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>?</td>
</tr>
<tr>
<td>Nr 10.0.3.5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>?</td>
</tr>
<tr>
<td>Nr 10.0.0.24</td>
<td>10.0.0.3</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>?</td>
</tr>
<tr>
<td>V* 10.0.2.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Vr 10.0.3.0/24</td>
<td>10.0.3.5</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>?</td>
</tr>
</tbody>
</table>
```

The table below describes the significant fields shown in the display.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the router.</td>
</tr>
<tr>
<td>Status codes</td>
<td>Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• s—The table entry is suppressed.</td>
</tr>
<tr>
<td></td>
<td>• d—The table entry is dampened.</td>
</tr>
<tr>
<td></td>
<td>• h—The table entry history.</td>
</tr>
<tr>
<td></td>
<td>• *—The table entry is valid.</td>
</tr>
<tr>
<td></td>
<td>• &gt;—The table entry is the best entry to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• i—The table entry was learned via an internal BGP (iBGP) session.</td>
</tr>
<tr>
<td></td>
<td>• r—The table entry is a RIB-failure.</td>
</tr>
<tr>
<td></td>
<td>• S—The table entry is stale.</td>
</tr>
<tr>
<td></td>
<td>• m—The table entry has multipath to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• b—The table entry has a backup path to use for that network.</td>
</tr>
<tr>
<td></td>
<td>• x—The table entry has a best external route to use for the network.</td>
</tr>
<tr>
<td>Origin codes</td>
<td>Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>• a—Path is selected as an additional path.</td>
</tr>
<tr>
<td></td>
<td>• i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a <strong>network</strong> router configuration command.</td>
</tr>
<tr>
<td></td>
<td>• e—Entry originated from an Exterior Gateway Protocol (EGP).</td>
</tr>
<tr>
<td></td>
<td>• ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.</td>
</tr>
<tr>
<td>RPKI validation codes</td>
<td>If shown, the RPKI validation state for the network prefix, which is downloaded from the RPKI server. The codes are shown only if the <strong>bgp rpki server</strong> or <strong>neighbor announce rpki state</strong> command is configured.</td>
</tr>
<tr>
<td>Network</td>
<td>IP address of a network entity.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.</td>
</tr>
<tr>
<td>Metric</td>
<td>If shown, the value of the interautonomous system metric.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LocPrf</td>
<td>Local preference value as set with the <code>set local-preference</code> route-map configuration command. The default value is 100.</td>
</tr>
<tr>
<td>Weight</td>
<td>Weight of the route as set via autonomous system filters.</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.</td>
</tr>
<tr>
<td>(stale)</td>
<td>Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.</td>
</tr>
<tr>
<td>Updated on</td>
<td>The time at which the path is received or updated.</td>
</tr>
</tbody>
</table>

**show ip bgp (4-Byte Autonomous System Numbers): Example**

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device#show ip bgp

BGP table version is 4, local router ID is 172.16.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network Next Hop Metric LocPrf Weight Path
* 10.1.1.0/24 192.168.1.2 0 0 65536 i
* 10.2.2.0/24 192.168.3.2 0 0 65550 i
* 172.16.1.0/24 0.0.0.0 0 32768 i
```

**show ip bgp network: Example**

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Device#show ip bgp 192.168.1.0

BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
    3
    10 10
      192.168.3.2 from 172.16.1.2 (10.2.2.2)
        Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
    10 10
      192.168.1.2 from 192.168.1.2 (10.3.3.3)
        Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:
Device#show ip bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
   Advertised to update-groups:
      1
         10.71.8.165 from 10.71.8.165 (192.168.0.102)
            Origin incomplete, localpref 100, valid, external, backup/repair
            Only allowed to recurse through connected route
      200
         10.71.11.165 from 10.71.11.165 (192.168.0.102)
            Origin incomplete, localpref 100, weight 100, valid, external, best
            Only allowed to recurse through connected route
      200
         10.71.10.165 from 10.71.10.165 (192.168.0.104)
            Origin incomplete, localpref 100, valid, external,
            Only allowed to recurse through connected route

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

**Table 128: show ip bgp ip-address Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP routing table entry for</td>
<td>IP address or network number of the routing table entry.</td>
</tr>
<tr>
<td>version</td>
<td>Internal version number of the table. This number is incremented whenever the table changes.</td>
</tr>
<tr>
<td>Paths</td>
<td>The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.</td>
</tr>
<tr>
<td>Multipath</td>
<td>This field is displayed when multipath load sharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.</td>
</tr>
<tr>
<td>Advertised to update-groups</td>
<td>The number of each update group for which advertisements are processed.</td>
</tr>
<tr>
<td>Origin</td>
<td>Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).</td>
</tr>
<tr>
<td>Extended Community</td>
<td>This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.</td>
</tr>
</tbody>
</table>

**show ip bgp all: Example**

The following is sample output from the `show ip bgp` command entered with the `all` keyword. Information about all configured address families is displayed.
Device#show ip bgp all

For address family: IPv4 Unicast *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>10.13.13.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>10.15.15.0/24</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>110.18.18.0/24</td>
<td>172.16.14.105</td>
<td>1388</td>
<td>91351</td>
<td>0</td>
<td>100 e</td>
</tr>
<tr>
<td>110.100.0/16</td>
<td>172.16.14.107</td>
<td>262</td>
<td>272</td>
<td>0</td>
<td>1 2 3 i</td>
</tr>
<tr>
<td>110.100.0/16</td>
<td>172.16.14.105</td>
<td>1388</td>
<td>91351</td>
<td>0</td>
<td>100 e</td>
</tr>
<tr>
<td>110.101.0/16</td>
<td>172.16.14.105</td>
<td>1388</td>
<td>91351</td>
<td>0</td>
<td>100 e</td>
</tr>
<tr>
<td>110.103.0/16</td>
<td>172.16.14.101</td>
<td>1388</td>
<td>173</td>
<td>173</td>
<td>100 e</td>
</tr>
<tr>
<td>110.104.0/16</td>
<td>172.16.14.101</td>
<td>1388</td>
<td>173</td>
<td>173</td>
<td>100 e</td>
</tr>
<tr>
<td>110.100.0/16</td>
<td>172.16.14.106</td>
<td>2219</td>
<td>20889</td>
<td>0</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td>110.101.0/16</td>
<td>172.16.14.106</td>
<td>2219</td>
<td>20889</td>
<td>0</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td>10.100.0/16</td>
<td>172.16.14.109</td>
<td>2309</td>
<td>200</td>
<td>300</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>172.16.14.108</td>
<td>1388</td>
<td>0</td>
<td>100</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>172.16.14.109</td>
<td>2309</td>
<td>200</td>
<td>300</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>172.16.14.108</td>
<td>1388</td>
<td>0</td>
<td>100</td>
<td>e</td>
</tr>
<tr>
<td></td>
<td>172.16.14.108</td>
<td>1388</td>
<td>0</td>
<td>100</td>
<td>e</td>
</tr>
<tr>
<td>192.168.5.0</td>
<td>0.0.0.0</td>
<td>0</td>
<td>32768</td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>10.80.0.0/16</td>
<td>172.16.14.108</td>
<td>1388</td>
<td>0</td>
<td>50</td>
<td>e</td>
</tr>
<tr>
<td>10.80.0.0/16</td>
<td>172.16.14.108</td>
<td>1388</td>
<td>0</td>
<td>50</td>
<td>e</td>
</tr>
</tbody>
</table>

For address family: VPNv4 Unicast *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
<tr>
<td></td>
<td>192.168.4.3</td>
<td>1622</td>
<td>0</td>
<td>100</td>
<td>53285 33299 51178 47751 e</td>
</tr>
</tbody>
</table>

For address family: IPv4 Multicast *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.40.40.0/26</td>
<td>172.16.14.110</td>
<td>2219</td>
<td>0</td>
<td>51178,47751,27016 e</td>
</tr>
<tr>
<td></td>
<td>10.1.1.1</td>
<td>1622</td>
<td>0</td>
<td>15 20 1 (2) e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.40.40.64/26</td>
<td>172.16.14.110</td>
<td>2219</td>
<td>0</td>
<td>51178,47751,27016 e</td>
</tr>
<tr>
<td></td>
<td>10.1.1.1</td>
<td>1622</td>
<td>0</td>
<td>15 20 1 (2) e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.40.40.128/26</td>
<td>172.16.14.110</td>
<td>2219</td>
<td>0</td>
<td>51178,47751,27016 e</td>
</tr>
<tr>
<td></td>
<td>10.1.1.1</td>
<td>1622</td>
<td>0</td>
<td>15 20 1 (2) e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>10.40.40.192/26</td>
<td>10.1.1.1</td>
<td>2563</td>
<td>0</td>
<td>15 20 1 (2) e</td>
</tr>
<tr>
<td></td>
<td>10.1.1.1</td>
<td>2563</td>
<td>0</td>
<td>15 20 1 (2) e</td>
<td></td>
</tr>
</tbody>
</table>
**show ip bgp longer-prefixes: Example**

The following is sample output from the `show ip bgp longer-prefixes` command:

```
Device#show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes
BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 10.92.0.0 10.92.72.30 8896 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.1.0 10.92.72.30 8796 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.11.0 10.92.72.30 42482 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.14.0 10.92.72.30 8976 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.15.0 10.92.72.30 8966 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.16.0 10.92.72.30 1400 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.17.0 10.92.72.30 1400 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.18.0 10.92.72.30 8976 32768 ?
  * 10.92.72.30 0 109 108 ?
*> 10.92.19.0 10.92.72.30 8976 32768 ?
  * 10.92.72.30 0 109 108 ?
```

**show ip bgp shorter-prefixes: Example**

The following is sample output from the `show ip bgp shorter-prefixes` command. An 8-bit prefix length is specified.

```
Device#show ip bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0 10.0.0.2 0 0 ?
  * 10.0.0.2 0 0 200 ?
```
**show ip bgp prefix-list: Example**

The following is sample output from the `show ip bgp prefix-list` command:

```
Device#show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 192.168.1.0</td>
<td>10.0.0.2</td>
<td></td>
<td></td>
<td></td>
<td>0 ?</td>
</tr>
<tr>
<td>*</td>
<td>10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>0 200 ?</td>
</tr>
</tbody>
</table>
```

**show ip bgp route-map: Example**

The following is sample output from the `show ip bgp route-map` command:

```
Device#show ip bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>*&gt; 192.168.1.0</td>
<td>10.0.0.2</td>
<td></td>
<td></td>
<td></td>
<td>0 ?</td>
</tr>
<tr>
<td>*</td>
<td>10.0.0.2</td>
<td>0</td>
<td>0</td>
<td>200</td>
<td>0 200 ?</td>
</tr>
</tbody>
</table>
```

**show ip bgp (Additional Paths): Example**

The following output indicates (for each neighbor) whether any of the additional path tags (group-best, all, best 2 or best 3) are applied to the path. A line of output indicates rx pathid (received from neighbor) and tx pathid (announcing to neighbors). Note that the “Path advertised to update-groups:” is now per-path when the BGP Additional Paths feature is enabled.

```
Device#show ip bgp 10.0.0.1 255.255.255.224

BGP routing table entry for 10.0.0.1/28, version 82
Paths: (10 available, best #5, table default)
Path advertised to update-groups: 21 25
Refresh Epoch 1
20 50, (Received from a RR-client)
  192.0.2.1 from 192.0.2.1 (192.0.2.1)
    Origin IGP, metric 200, localpref 100, valid, internal, all
    Originator: 192.0.2.1, Cluster list: 2.2.2.2
    mpls labels in/out 16/nolabel
    rx pathid: 0, tx pathid: 0x9
    Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups: 18 21
Refresh Epoch 1
30
  192.0.2.2 from 192.0.2.2 (192.0.2.2)
    Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Originator: 192.0.2.2, Cluster list: 4.4.4.4
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x8
Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
16 18 19 20 21 22 24
25 27
Refresh Epoch 1
10
192.0.2.3 from 192.0.2.3 (192.0.2.3)
Origin IGP, metric 200, localpref 100, valid, external, best2, all
mpls labels in/out 16/nolabel
rx pathid: 0, tx pathid: 0x7
Updated on Aug 14 2018 18:30:39 PST
Path advertised to update-groups:
20 21 22 24 25
Refresh Epoch 1
10
192.0.2.4 from 192.0.2.4 (192.0.2.4)
Origin IGP, metric 300, localpref 100, valid, external, best3, all
mpls labels in/out 16/nolabel
rx pathid: 0, tx pathid: 0x6
Updated on Jun 17 2018 11:12:30 PST
Path advertised to update-groups:
10 13 17 18 19 20 21
22 23 24 25 26 27 28
Refresh Epoch 1
10
192.0.2.5 from 192.0.2.5 (192.0.2.5)
Origin IGP, metric 100, localpref 100, valid, external, best
mpls labels in/out 16/nolabel
rx pathid: 0, tx pathid: 0x0
Updated on Jun 17 2018 11:12:30 PST
Path advertised to update-groups:
18 23 24 25 26 27 28
Refresh Epoch 1
30
192.0.2.6 from 192.0.2.6 (192.0.2.6)
Origin IGP, metric 200, localpref 100, valid, internal, all
Originator: 192.0.2.6, Cluster list: 5.5.5.5
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x5
Updated on Jun 17 2018 11:12:30 PST
Path advertised to update-groups:
18 23 24 26 28
Refresh Epoch 1
60 40, (Received from a RR-client)
192.0.2.7 from 192.0.2.7 (192.0.2.7)
Origin IGP, metric 250, localpref 100, valid, internal, group-best
Originator: 192.0.2.7, Cluster list: 3.3.3.3
mpls labels in/out 16/nolabel
rx pathid: 0x2, tx pathid: 0x2
Updated on Jun 17 2018 11:12:30 PST
Path advertised to update-groups:
25
Refresh Epoch 1
30 40, (Received from a RR-client)
192.0.2.8 from 192.0.2.8 (192.0.2.8)
Origin IGP, metric 200, localpref 100, valid, internal, all
Originator: 192.0.2.8, Cluster list: 2.2.2.2
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x3
Updated on Jun 17 2018 11:12:30 PST
Path advertised to update-groups:
show ip bgp network (BGP Attribute Filter): Example

The following is sample output from the **show ip bgp** command that displays unknown and discarded path attributes:

```
Device#show ip bgp 192.0.2.0/32
BGP routing table entry for 192.0.2.0/32, version 0
Paths: (1 available, no best path)
  Refresh Epoch 1
    Local
      192.168.101.2 from 192.168.101.2 (192.168.101.2)
        Origin IGP, localpref 100, valid, internal
        unknown transitive attribute: flag 0xE0 type 0x81 length 0x20
          value 0000 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000 0000
        unknown transitive attribute: flag 0xE0 type 0x83 length 0x20
          value 0000 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000 0000
        discarded unknown attribute: flag 0x40 type 0x63 length 0x64
          value 0000 0000 0000 0000 0000 0000 0000 0000
          0000 0000 0000 0000 0000 0000 0000 0000
```

show ip bgp version: Example

The following is sample output from the **show ip bgp version** command:

```
Device#show ip bgp version
BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, R RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
  *> 192.168.34.2/24 10.0.0.1 0 0 1 ?
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following example shows how to display the network version:

```
Device# show ip bgp 192.168.34.2 | include version
```

BGP routing table entry for 192.168.34.2/24, version 5

The following sample output from the `show ip bgp version recent` command displays the prefix changes in the specified version:

```
Device# show ip bgp version recent 2
```

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

<table>
<thead>
<tr>
<th>Network</th>
<th>Next Hop</th>
<th>Metric</th>
<th>LocPrf</th>
<th>Weight</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.134.1/28</td>
<td>10.0.0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1?</td>
</tr>
<tr>
<td>192.168.134.19/28</td>
<td>10.0.0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1?</td>
</tr>
<tr>
<td>192.168.134.34/28</td>
<td>10.0.0.1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1?</td>
</tr>
</tbody>
</table>

The following sample output for the `show ip bgp summary` command shows the peak watermarks and their time-stamps for the peak number of route entries per neighbor bases:

```
Device# show ip bgp 80.230.70.96 best-path-reason
```

BGP routing table entry for 192.168.3.0/24, version 72
Paths: (2 available, best #2, table default)
Advertised to update-groups:
2
Refresh Epoch 1
2
  10.0.101.1 from 10.0.101.1 (10.0.101.1)
  Origin IGP, localpref 100, valid, external
  Extended Community: RT:100:100
  rx pathid: 0, tx pathid: 0
  Updated on Aug 14 2018 18:34:12 PST
  Best Path Evaluation: Path is younger

Refresh Epoch 1
1
  10.0.96.254 from 10.0.96.254 (10.0.96.254)
  Origin IGP, localpref 100, valid, external, best
  rx pathid: 0, tx pathid: 0x0
  Updated on Aug 14 2018 18:30:39 PST
  Best Path Evaluation: Overall best path

The following sample output for the `show ip bgp summary` command shows the peak watermarks and their time-stamps for the peak number of route entries per neighbor bases:
For address family: L2VPN E-VPN
BGP router identifier 10.10.10.10, local AS number 1
BGP table version is 183, main routing table version 183
2 network entries using 688 bytes of memory
2 path entries using 416 bytes of memory
2/2 BGP path/bestpath attribute entries using 560 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1688 total bytes of memory
BGP activity 58/54 prefixes, 110/106 paths, scan interval 60 secs
30 networks peaked at 00:35:36 Jul 28 2018 PST (00:00:47.321 ago)

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp asnotation dot</td>
<td>Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.</td>
</tr>
<tr>
<td>clear ip bgp</td>
<td>Resets BGP connections using hard or soft reconfiguration.</td>
</tr>
<tr>
<td>ip bgp community new-format</td>
<td>Configures BGP to display communities in the format AA:NN.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Creates a prefix list or adds a prefix-list entry.</td>
</tr>
<tr>
<td>route-map</td>
<td>Defines the conditions for redistributing routes from one routing protocol into another routing protocol.</td>
</tr>
<tr>
<td>router bgp</td>
<td>Configures the BGP routing process.</td>
</tr>
</tbody>
</table>
show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the `show ip bgp neighbors` command in user or privileged EXEC mode.

```
show ip bgp [ipv4 {multicast | unicast} | vpnv4 all | vpnv6 unicast all] [slow|ip-address | ipv6-address] [advertised-routes | dampened-routes | flap-statistics | paths [reg-exp] | policy [detail] | received prefix-filter | received-routes | routes]]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Displays peers in the IPv4 address family.</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Specifies IPv4 multicast address prefixes.</td>
</tr>
<tr>
<td>unicast</td>
<td>(Optional) Specifies IPv4 unicast address prefixes.</td>
</tr>
<tr>
<td>vpnv4 all</td>
<td>(Optional) Displays peers in the VPNv4 address family.</td>
</tr>
<tr>
<td>vpnv6 unicast all</td>
<td>(Optional) Displays peers in the VPNv6 address family.</td>
</tr>
<tr>
<td>slow</td>
<td>(Optional) Displays information about dynamically configured slow peers.</td>
</tr>
<tr>
<td>ip-address</td>
<td>(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>(Optional) IP address of the IPv6 neighbor.</td>
</tr>
<tr>
<td>advertised-routes</td>
<td>(Optional) Displays all routes that have been advertised to neighbors.</td>
</tr>
<tr>
<td>dampened-routes</td>
<td>(Optional) Displays the dampened routes received from the specified neighbor.</td>
</tr>
<tr>
<td>flap-statistics</td>
<td>(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).</td>
</tr>
<tr>
<td>paths reg-exp</td>
<td>(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.</td>
</tr>
<tr>
<td>policy</td>
<td>(Optional) Displays the policies applied to this neighbor per address family.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.</td>
</tr>
<tr>
<td>received prefix-filter</td>
<td>(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.</td>
</tr>
<tr>
<td>received-routes</td>
<td>(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.</td>
</tr>
<tr>
<td>routes</td>
<td>(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the <code>received-routes</code> keyword.</td>
</tr>
</tbody>
</table>
The output of this command displays information for all neighbors.

### Command Modes

- User EXEC (>)
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>BGP Peak Prefix Watermark was added to the command output.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Use the `show ip bgp neighbors` command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

### Examples

Example output is different for the various keywords available for the `show ip bgp neighbors` command. Examples using the various keywords appear in the following sections.

#### show ip bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
  60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
    Sent   Rcvd
    Opens:  3   3
    Notifications: 0   0
    Updates:  0   0
    Keepalives: 113   112
    Route Refresh: 0   0
    Total:  116   115
  Default minimum time between advertisement runs is 5 seconds
  For address family: IPv4 Unicast
    BGP additional-paths computation is enabled
```
BGP advertise-best-external is enabled
BGP table version 1, neighbor version 1/0
Output queue size : 0
Index 1, Offset 0, Mask Ox2
1 update-group member

Prefix activity:  
Sent  |  Rcvd  
Prepending  |  0  |  0  
Prefixes Total:  |  0  |  0  
Implicit Withdraw:  |  0  |  0  
Explicit Withdraw:  |  0  |  0  
Used as bestpath:  | n/a  |  0  
Used as multipath:  | n/a  |  0  
Outbound  |  Inbound  
Local Policy Denied Prefixes:  |  0  |  0  
Total:  |  0  |  0  

Number of NLRI in the update sent: max 0, min 0
Connections established 3; dropped 2
Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
<table>
<thead>
<tr>
<th>Timer</th>
<th>Starts</th>
<th>Wakeups</th>
<th>Next</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retrans</td>
<td>27</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>TimeWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>AckHold</td>
<td>27</td>
<td>18</td>
<td>0x0</td>
</tr>
<tr>
<td>SendWnd</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>GiveUp</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
<tr>
<td>DeadWait</td>
<td>0</td>
<td>0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

iass: 3915509457 snduna: 3915510016 sndnxt: 3915510016 sndwnd: 15826
irs: 233567076 rcvnxn: 233567616 rcvwnd: 15845 delrcvwnd: 539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

**Table 129: show ip bgp neighbors Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP neighbor</td>
<td>IP address of the BGP neighbor and its autonomous system number.</td>
</tr>
<tr>
<td>remote AS</td>
<td>Autonomous system number of the neighbor.</td>
</tr>
<tr>
<td>local AS 300 no-prepend (not shown in display)</td>
<td>Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>internal link</td>
<td>“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.</td>
</tr>
<tr>
<td>BGP version</td>
<td>BGP version being used to communicate with the remote router.</td>
</tr>
<tr>
<td>remote router ID</td>
<td>IP address of the neighbor.</td>
</tr>
<tr>
<td>BGP state</td>
<td>Finite state machine (FSM) stage of session negotiation.</td>
</tr>
<tr>
<td>up for</td>
<td>Time, in hh:mm:ss, that the underlying TCP connection has been in existence.</td>
</tr>
<tr>
<td>Last read</td>
<td>Time, in hh:mm:ss, since BGP last received a message from this neighbor.</td>
</tr>
<tr>
<td>last write</td>
<td>Time, in hh:mm:ss, since BGP last sent a message to this neighbor.</td>
</tr>
<tr>
<td>hold time</td>
<td>Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.</td>
</tr>
<tr>
<td>keepalive interval</td>
<td>Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.</td>
</tr>
<tr>
<td>Neighbor capabilities</td>
<td>BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers.</td>
</tr>
<tr>
<td>Route refresh</td>
<td>Status of the route refresh capability.</td>
</tr>
<tr>
<td>MPLS Label capability</td>
<td>Indicates that MPLS labels are both sent and received by the eBGP peer.</td>
</tr>
<tr>
<td>Graceful Restart Capability</td>
<td>Status of the graceful restart capability.</td>
</tr>
<tr>
<td>Address family IPv4 Unicast</td>
<td>IP Version 4 unicast-specific properties of this neighbor.</td>
</tr>
<tr>
<td>Message statistics</td>
<td>Statistics organized by message type.</td>
</tr>
<tr>
<td>InQ depth is</td>
<td>Number of messages in the input queue.</td>
</tr>
<tr>
<td>OutQ depth is</td>
<td>Number of messages in the output queue.</td>
</tr>
<tr>
<td>Sent</td>
<td>Total number of transmitted messages.</td>
</tr>
<tr>
<td>Revd</td>
<td>Total number of received messages.</td>
</tr>
<tr>
<td>Opens</td>
<td>Number of open messages sent and received.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Number of notification (error) messages sent and received.</td>
</tr>
<tr>
<td>Updates</td>
<td>Number of update messages sent and received.</td>
</tr>
<tr>
<td>Keepalives</td>
<td>Number of keepalive messages sent and received.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Route Refresh</td>
<td>Number of route refresh request messages sent and received.</td>
</tr>
<tr>
<td>Total</td>
<td>Total number of messages sent and received.</td>
</tr>
<tr>
<td>Default minimum time between</td>
<td>Time, in seconds, between advertisement transmissions.</td>
</tr>
<tr>
<td>For address family:</td>
<td>Address family to which the following fields refer.</td>
</tr>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.</td>
</tr>
<tr>
<td>neighbor version</td>
<td>Number used by the software to track prefixes that have been sent and those that need to be sent.</td>
</tr>
<tr>
<td>1 update-group member</td>
<td>Number of the update-group member for this address family.</td>
</tr>
<tr>
<td>Prefix activity</td>
<td>Prefix statistics for this address family.</td>
</tr>
<tr>
<td>Prefixes Current</td>
<td>Number of prefixes accepted for this address family.</td>
</tr>
<tr>
<td>Prefixes Total</td>
<td>Total number of received prefixes.</td>
</tr>
<tr>
<td>Implicit Withdraw</td>
<td>Number of times that a prefix has been withdrawn and readvertised.</td>
</tr>
<tr>
<td>Explicit Withdraw</td>
<td>Number of times that a prefix has been withdrawn because it is no longer feasible.</td>
</tr>
<tr>
<td>Used as bestpath</td>
<td>Number of received prefixes installed as best paths.</td>
</tr>
<tr>
<td>Used as multipath</td>
<td>Number of received prefixes installed as multipaths.</td>
</tr>
<tr>
<td>* Saved (soft-reconfig)</td>
<td>Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>* History paths</td>
<td>This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>* Invalid paths</td>
<td>Number of invalid paths. This field is displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>Local Policy Denied Prefixes</td>
<td>Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.</td>
</tr>
<tr>
<td>* route-map</td>
<td>Displays inbound and outbound route-map policy denials.</td>
</tr>
<tr>
<td>* filter-list</td>
<td>Displays inbound and outbound filter-list policy denials.</td>
</tr>
<tr>
<td>* prefix-list</td>
<td>Displays inbound and outbound prefix-list policy denials.</td>
</tr>
<tr>
<td>* Ext Community</td>
<td>Displays only outbound extended community policy denials.</td>
</tr>
<tr>
<td>* AS_PATH too long</td>
<td>Displays outbound AS_PATH length policy denials.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>* AS_PATH loop</td>
<td>Displays outbound AS_PATH loop policy denials.</td>
</tr>
<tr>
<td>* AS_PATH confed info</td>
<td>Displays outbound confederation policy denials.</td>
</tr>
<tr>
<td>* AS_PATH contains AS 0</td>
<td>Displays outbound denials of autonomous system 0.</td>
</tr>
<tr>
<td>* NEXT_HOP Martian</td>
<td>Displays outbound martian denials.</td>
</tr>
<tr>
<td>* NEXT_HOP non-local</td>
<td>Displays outbound nonlocal next-hop denials.</td>
</tr>
<tr>
<td>* NEXT_HOP is us</td>
<td>Displays outbound next-hop-self denials.</td>
</tr>
<tr>
<td>* CLUSTER_LIST loop</td>
<td>Displays outbound cluster-list loop denials.</td>
</tr>
<tr>
<td>* ORIGINATOR loop</td>
<td>Displays outbound denials of local originated routes.</td>
</tr>
<tr>
<td>* unsuppress-map</td>
<td>Displays inbound denials due to an unsuppress map.</td>
</tr>
<tr>
<td>* advertise-map</td>
<td>Displays inbound denials due to an advertise map.</td>
</tr>
<tr>
<td>* VPN Imported prefix</td>
<td>Displays inbound denials of VPN prefixes.</td>
</tr>
<tr>
<td>* Well-known Community</td>
<td>Displays inbound denials of well-known communities.</td>
</tr>
<tr>
<td>* SOO loop</td>
<td>Displays inbound denials due to site-of-origin.</td>
</tr>
<tr>
<td>* Bestpath from this peer</td>
<td>Displays inbound denials because the best path came from the local router.</td>
</tr>
<tr>
<td>* Suppressed due to dampening</td>
<td>Displays inbound denials because the neighbor or link is in a dampening state.</td>
</tr>
<tr>
<td>* Bestpath from iBGP peer</td>
<td>Deploys inbound denials because the best path came from an iBGP neighbor.</td>
</tr>
<tr>
<td>* Incorrect RIB for CE</td>
<td>Deploys inbound denials due to RIB errors for a customer edge (CE) router.</td>
</tr>
<tr>
<td>* BGP distribute-list</td>
<td>Displays inbound denials due to a distribute list.</td>
</tr>
<tr>
<td>Number of NLRIs...</td>
<td>Number of network layer reachability attributes in updates.</td>
</tr>
<tr>
<td>Current session network count</td>
<td>Displays the peak number of networks observed in the current session.</td>
</tr>
<tr>
<td>peaked...</td>
<td></td>
</tr>
<tr>
<td>Highest network count observed</td>
<td>Displays the peak number of networks observed since startup.</td>
</tr>
<tr>
<td>at...</td>
<td></td>
</tr>
<tr>
<td>Connections established</td>
<td>Number of times a TCP and BGP connection has been successfully established.</td>
</tr>
<tr>
<td>dropped</td>
<td>Number of times that a valid session has failed or been taken down.</td>
</tr>
<tr>
<td>Last reset</td>
<td>Time, in hh:mm:ss, since this peering session was last reset. The reason for</td>
</tr>
<tr>
<td></td>
<td>the reset is displayed on this line.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>External BGP neighbor may be...</td>
<td>Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.</td>
</tr>
<tr>
<td>Connection state</td>
<td>Connection status of the BGP peer.</td>
</tr>
<tr>
<td>unread input bytes</td>
<td>Number of bytes of packets still to be processed.</td>
</tr>
<tr>
<td>Connection is ECN Disabled</td>
<td>Explicit congestion notification status (enabled or disabled).</td>
</tr>
<tr>
<td>Local host: 10.108.50.1, Local port: 179</td>
<td>IP address of the local BGP speaker. BGP port number 179.</td>
</tr>
<tr>
<td>Foreign host: 10.108.50.2, Foreign port: 42698</td>
<td>Neighbor address and BGP destination port number.</td>
</tr>
<tr>
<td>Enqueued packets for retransmit:</td>
<td>Packets queued for retransmission by TCP.</td>
</tr>
<tr>
<td>Event Timers</td>
<td>TCP event timers. Counters are provided for starts and wakeups (expired timers).</td>
</tr>
<tr>
<td>Retrans</td>
<td>Number of times a packet has been retransmitted.</td>
</tr>
<tr>
<td>TimeWait</td>
<td>Time waiting for the retransmission timers to expire.</td>
</tr>
<tr>
<td>AckHold</td>
<td>Acknowledgment hold timer.</td>
</tr>
<tr>
<td>SendWnd</td>
<td>Transmission (send) window.</td>
</tr>
<tr>
<td>KeepAlive</td>
<td>Number of keepalive packets.</td>
</tr>
<tr>
<td>GiveUp</td>
<td>Number of times a packet is dropped due to no acknowledgment.</td>
</tr>
<tr>
<td>PmtuAger</td>
<td>Path MTU discovery timer.</td>
</tr>
<tr>
<td>DeadWait</td>
<td>Expiration timer for dead segments.</td>
</tr>
<tr>
<td>iss:</td>
<td>Initial packet transmission sequence number.</td>
</tr>
<tr>
<td>snduna:</td>
<td>Last transmission sequence number that has not been acknowledged.</td>
</tr>
<tr>
<td>sndnxt:</td>
<td>Next packet sequence number to be transmitted.</td>
</tr>
<tr>
<td>sndwnd:</td>
<td>TCP window size of the remote neighbor.</td>
</tr>
<tr>
<td>irs:</td>
<td>Initial packet receive sequence number.</td>
</tr>
<tr>
<td>rcvnxt:</td>
<td>Last receive sequence number that has been locally acknowledged.</td>
</tr>
<tr>
<td>rcvwnd:</td>
<td>TCP window size of the local host.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>delrcvwnd:</td>
<td>Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is higher than a full-sized packet, at which point it is applied to the rcvwnd field.</td>
</tr>
<tr>
<td>SRTT:</td>
<td>A calculated smoothed round-trip timeout.</td>
</tr>
<tr>
<td>RTTO:</td>
<td>Round-trip timeout.</td>
</tr>
<tr>
<td>RTV:</td>
<td>Variance of the round-trip time.</td>
</tr>
<tr>
<td>KRTT:</td>
<td>New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.</td>
</tr>
<tr>
<td>minRTT:</td>
<td>Shortest recorded round-trip timeout (hard-wire value used for calculation).</td>
</tr>
<tr>
<td>maxRTT:</td>
<td>Longest recorded round-trip timeout.</td>
</tr>
<tr>
<td>ACK hold:</td>
<td>Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.</td>
</tr>
<tr>
<td>IP Precedence value:</td>
<td>IP precedence of the BGP packets.</td>
</tr>
<tr>
<td>Datagrams</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>Rcvd:</td>
<td>Number of received packets.</td>
</tr>
<tr>
<td>out of order:</td>
<td>Number of packets received out of sequence.</td>
</tr>
<tr>
<td>with data</td>
<td>Number of update packets sent with data.</td>
</tr>
<tr>
<td>total data bytes</td>
<td>Total amount of data received, in bytes.</td>
</tr>
<tr>
<td>Sent</td>
<td>Number of update packets sent.</td>
</tr>
<tr>
<td>Second Congestion</td>
<td>Number of update packets with data sent.</td>
</tr>
<tr>
<td>Datagrams: Rcvd</td>
<td>Number of update packets received from a neighbor.</td>
</tr>
<tr>
<td>retransmit</td>
<td>Number of packets retransmitted.</td>
</tr>
<tr>
<td>fastretransmit</td>
<td>Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.</td>
</tr>
<tr>
<td>partialack</td>
<td>Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).</td>
</tr>
<tr>
<td>Second Congestion</td>
<td>Number of second retransmissions sent due to congestion.</td>
</tr>
</tbody>
</table>
**show ip bgp neighbors (4-Byte Autonomous System Numbers)**

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Device# show ip bgp neighbors
BGP neighbor is 192.168.1.2, remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70 seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds

BGP neighbor is 192.168.3.2, remote AS 65550, external link
  Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70 seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

**show ip bgp neighbors advertised-routes**

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network  Next Hop  Metric  LocPrf  Weight  Path
*>10.0.0.0  172.16.232.179  0  100  0  ?
*> 10.20.2.0  10.0.0.0  0  32768 1
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BGP table version</td>
<td>Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.</td>
</tr>
<tr>
<td>local router ID</td>
<td>IP address of the local BGP speaker.</td>
</tr>
</tbody>
</table>
### Field Description

**Status codes**

Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values:

- **s**—The table entry is suppressed.
- **d**—The table entry is dampened and will not be advertised to BGP neighbors.
- **h**—The table entry does not contain the best path based on historical information.
- *****—The table entry is valid.
- **>**—The table entry is the best entry to use for that network.
- **i**—The table entry was learned via an internal BGP (iBGP) session.

**Origin codes**

Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values:

- **i**—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a `network` router configuration command.
- **e**—Entry originated from Exterior Gateway Protocol (EGP).
- **?**—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.

**Network**

IP address of a network entity.

**Next Hop**

IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.

**Metric**

If shown, this is the value of the interautonomous system metric. This field is not used frequently.

**LocPrf**

Local preference value as set with the `set local-preference` route-map configuration command. The default value is 100.

**Weight**

Weight of the route as set via autonomous system filters.

**Path**

Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

---

### show ip bgp neighbors check-control-plane-failure

The following is sample output from the `show ip bgp neighbors` command entered with the `check-control-plane-failure` option configured:

```
Device#show ip bgp neighbors 10.10.10.1

BGP neighbor is 10.10.10.1, remote AS 10, internal link
Fall over configured for session
BFD is configured. BFD peer is Up. Using BFD to detect fast failover (single-hop) with c-bit check-control-plane-failure.
```
Inherits from template cbit-tps for session parameters
BGP version 4, remote router ID 10.7.7.7
BGP state = Established, up for 00:03:55
Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds

Neighbor sessions:
1 active, is not multisection capable (disabled)
Neighbor capabilities:
Route refresh: advertised and received(new)
Four-octets ASN Capability: advertised and received
Address family IPv4 Unicast: advertised and received
Enhanced Refresh Capability: advertised and received
Multisection Capability:
Stateful switchover support enabled: NO for session 1

**show ip bgp neighbors paths**

The following is sample output from the `show ip bgp neighbors` command entered with the `paths` keyword:

```
Device#show ip bgp neighbors 172.29.232.178 paths 10
Address Refcount Metric Path
0x60E577B0 2 40 10 ?
```

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

**Table 131: show ip bgp neighbors paths Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Internal address where the path is stored.</td>
</tr>
<tr>
<td>Refcount</td>
<td>Number of routes using that path.</td>
</tr>
<tr>
<td>Metric</td>
<td>Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)</td>
</tr>
<tr>
<td>Path</td>
<td>Autonomous system path for that route, followed by the origin code for that route.</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors received prefix-filter**

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device#show ip bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32
```

The table below describes the significant fields shown in the display.
Table 132: show ip bgp neighbors received prefix-filter Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address family</td>
<td>Address family mode in which the prefix filter is received.</td>
</tr>
<tr>
<td>ip prefix-list</td>
<td>Prefix list sent from the specified neighbor.</td>
</tr>
</tbody>
</table>

**show ip bgp neighbors policy**

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited polices are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device#show ip bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
  route-map ROUTE in
Inherited polices:
  prefix-list NO-MARKETING in
  route-map ROUTE in
  weight 300
  maximum-prefix 10000
```

**BGP Attribute Filter and Enhanced Attribute Error Handling**

The following is sample output from the `show ip bgp neighbors` command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```
Device#show ip bgp vpnv4 all neighbors 10.0.103.1
BGP neighbor is 10.0.103.1, remote AS 100, internal link
Path-attribute treat-as-withdraw inbound
Path-attribute treat-as-withdraw value 128
Path-attribute treat-as-withdraw 128 in: count 2
Path-attribute discard 128 inbound
Path-attribute discard 128 in: count 2

<table>
<thead>
<tr>
<th>Outbound</th>
<th>Inbound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Policy Denied Prefixes:</td>
<td>--------</td>
</tr>
<tr>
<td>MALFORM treat as withdraw:</td>
<td>0</td>
</tr>
<tr>
<td>Total:</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**BGP Additional Paths**

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```
Device#show ip bgp neighbors 10.108.50.2
```
BGP neighbor is 10.108.50.2, remote AS 1, internal link
BGP version 4, remote router ID 192.168.252.252
BGP state = Established, up for 00:24:25
Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:
Additional paths Send: advertised and received
Additional paths Receive: advertised and received
Route refresh: advertised and received(old & new)
Graceful Restart Capability: advertised and received
Address family IPv4 Unicast: advertised and received

BGP—Multiple Cluster IDs

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user's input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

Device# show ip bgp neighbors 192.168.2.2 | i cluster-id

Configured with the cluster-id 192.168.15.6

BGP Peak Prefix Watermark

The following sample output shows the peak watermarks and their timestamps displayed for the peak number of route entries per neighbor bases:

Device# show ip bgp ipv4 unicast neighbors 11.11.11.11

BGP neighbor is 11.11.11.11, remote AS 1, internal link
BGP version 4, remote router ID 0.0.0.0
BGP state = Idle, down for 00:01:43
Neighbor sessions:
0 active, is not multisession capable (disabled)
Stateful switchover support enabled: NO
Do log neighbor state changes (via global configuration)
Default minimum time between advertisement runs is 0 seconds
For address family: IPv4 Unicast
BGP table version 27, neighbor version 1/27
Output queue size : 0
Index 0, Advertise bit 0
Slow-peer detection is disabled
Slow-peer split-update-group dynamic is disabled

<table>
<thead>
<tr>
<th>Prefix activity:</th>
<th>Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prefixes Current:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prefixes Total:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Implicit Withdraw:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Explicit Withdraw:</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Used as bestpath:</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td>Used as multipath:</td>
<td>n/a</td>
<td>0</td>
</tr>
<tr>
<td>Used as secondary:</td>
<td>n/a</td>
<td>0</td>
</tr>
</tbody>
</table>

Outbound Inbound
Local Policy Denied Prefixes: | 0 | 0 |
Total: | 0 | 0 |
Number of NLRIs in the update sent: max 2, min 0
Current session network count peaked at 20 entries at 00:00:23 Aug 8 2018 PST (00:01:29.156 ago).
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Refresh Epoch: 1
Last Sent Refresh Start-of-rib: never
Last Sent Refresh End-of-rib: never
Last Received Refresh Start-of-rib: never
Last Received Refresh End-of-rib: never

<table>
<thead>
<tr>
<th>Refresh activity:</th>
<th>Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Start-of-RIB</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Refresh End-of-RIB</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

BGP Soft Inbound and Outbound Refresh Time

In the following example, the times of occurrence of the soft inbound and outbound refresh, to or from the given neighbour, are displayed:

Device#show ip bgp l2vpn evpn neighbors 11.11.11.11

BGP neighbor is 11.11.11.11, remote AS 1, internal link
BGP version 4, remote router ID 11.11.11.11
BGP state = Established, up for 00:14:06
Last read 00:00:21, last write 00:00:28, hold time is 180, keepalive
............
Do log neighbor state changes (via global configuration)
Default minimum time between advertisement runs is 0 seconds

For address family: L2VPN E-VPN
Session: 11.11.11.11
BGP table version 30, neighbor version 30/0
Output queue size : 0
Index 1, Advertise bit 0
1 update-group member
Community attribute sent to this neighbor
Extended-community attribute sent to this neighbor
............
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Refresh Epoch: 2
Last Sent Refresh Start-of-rib: never
Last Sent Refresh End-of-rib: never
Last Received Refresh Start-of-rib: 00:14:06
Last Received Refresh End-of-rib: 00:14:06
Refresh-In took 0 seconds

<table>
<thead>
<tr>
<th>Refresh activity:</th>
<th>Sent</th>
<th>Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Start-of-RIB</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Refresh End-of-RIB</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

Address tracking is enabled, the RIB does have a route to 11.11.11.11
Route to peer address reachability Up: 1; Down: 0
Last notification 00:14:07
Connections established 1; dropped 0

............
Packets received in fast path: 0, fast processed: 0, slow path: 0
fast lock acquisition failures: 0, slow path: 0
TCP Semaphore 0x7FA8A0AE7BA0 FREE

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp asnotation dot</td>
<td>Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.</td>
</tr>
<tr>
<td>bgp enhanced-error</td>
<td>Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.</td>
</tr>
<tr>
<td>neighbor path-attribute discard</td>
<td>Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.</td>
</tr>
<tr>
<td>neighbor path-attribute treat-as-withdraw</td>
<td>Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.</td>
</tr>
<tr>
<td>neighbor send-label</td>
<td>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</td>
</tr>
<tr>
<td>neighbor send-label explicit-null</td>
<td>Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.</td>
</tr>
<tr>
<td>router bgp</td>
<td>Configures the BGP routing process.</td>
</tr>
</tbody>
</table>
show ip eigrp interfaces

To display information about interfaces that are configured for the Enhanced Interior Gateway Routing Protocol (EIGRP), use the `show ip eigrp interfaces` command in user EXEC or privileged EXEC mode.

```
show ip eigrp [vrf vrf-name] [autonomous-system-number] interfaces [type number] [{detail}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Displays information about the specified virtual routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>autonomous-system-number</td>
<td>(Optional) Autonomous system number whose output needs to be filtered.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed information about EIGRP interfaces for a specific EIGRP process.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ip eigrp interfaces` command to display active EIGRP interfaces and EIGRP-specific interface settings and statistics. The optional `type number` argument and the `detail` keyword can be entered in any order.

If an interface is specified, only information about that interface is displayed. Otherwise, information about all interfaces on which EIGRP is running is displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

This command can be used to display information about EIGRP named and EIGRP autonomous system configurations.

This command displays the same information as the `show eigrp address-family interfaces` command. Cisco recommends using the `show eigrp address-family interfaces` command.

**Examples**

The following is sample output from the `show ip eigrp interfaces` command:

```
Device#show ip eigrp interfaces
EIGRP-IPv4 Interfaces for AS(60)
   Xmit Queue   Mean   Pacing Time   Multicast   Pending
```
The following sample output from the `show ip eigrp interfaces detail` command displays detailed information about all active EIGRP interfaces:

Device#`show ip eigrp interfaces detail`

EIGRP-IPv4 Interfaces for AS(1)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Un/Reliable</th>
<th>SRTT</th>
<th>Un/Reliable</th>
<th>Flow Timer</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Et0/0</td>
<td>1</td>
<td>0/0</td>
<td>0</td>
<td>0/0</td>
<td>525</td>
<td>0</td>
</tr>
</tbody>
</table>

Hello-interval is 5, Hold-time is 15
Split-horizon is enabled
Next xmit serial <none>
Packetized sent/expedited: 3/0
Hello's sent/expedited: 6/2
Un/reliable mcasts: 0/6 Un/reliable ucasts: 7/4
Mcast exceptions: 1 CR packets: 1 ACKs suppressed: 0
Retransmissions sent: 1 Out-of-sequence rcvd: 0
Topology-ids on interface - 0
Authentication mode is not set

The following sample output from the `show ip eigrp interfaces detail` command displays detailed information about a specific interface on which the `no ip next-hop self` command is configured along with the `no-ecmp-mode` option:

Device#`show ip eigrp interfaces detail tunnel 0`

EIGRP-IPv4 Interfaces for AS(1)

<table>
<thead>
<tr>
<th>Interface</th>
<th>Peers</th>
<th>Un/Reliable</th>
<th>SRTT</th>
<th>Un/Reliable</th>
<th>Flow Timer</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tu0/0</td>
<td>2</td>
<td>0/0</td>
<td>0/0</td>
<td>0</td>
<td>50</td>
<td>0</td>
</tr>
</tbody>
</table>

Hello-interval is 5, Hold-time is 15
Split-horizon is disabled
Next xmit serial <none>
Packetized sent/expedited: 24/3
Hello's sent/expedited: 28083/9
Un/reliable mcasts: 0/19 Un/reliable ucasts: 18/64
Mcast exceptions: 5 CR packets: 5 ACKs suppressed: 0
Retransmissions sent: 52 Out-of-sequence rcvd: 2
Next-hop-self disabled, next-hop info forwarded, **ECMP mode Enabled**
Topology-ids on interface - 0
Authentication mode is not set

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

**Table 133: show ip eigrp interfaces Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface on which EIGRP is configured.</td>
</tr>
<tr>
<td>Peers</td>
<td>Number of directly connected EIGRP neighbors.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
PeerQ Un/Reliable | Number of unreliable and reliable packets queued for transmission to specific peers on the interface.
Xmit Queue Un/Reliable | Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT | Mean smooth round-trip time (SRTT) interval (in seconds).
Pacing Time Un/Reliable | Pacing time (in seconds) used to determine when EIGRP packets (unreliable and reliable) should be sent out of the interface.
Multicast Flow Timer | Maximum number of seconds for which the device will send multicast EIGRP packets.
Pending Routes | Number of routes in the transmit queue waiting to be sent.
Packetized sent/expedited | Number of EIGRP routes that have been prepared for sending packets to neighbors on an interface, and the number of times multiple routes were stored in a single packet.
Hello’s sent/expedited | Number of EIGRP hello packets that have been sent on an interface and packets that were expedited.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show eigrp address-family interfaces</strong></td>
<td>Displays information about address family interfaces configured for EIGRP.</td>
</tr>
<tr>
<td><strong>show ip eigrp neighbors</strong></td>
<td>Displays neighbors discovered by EIGRP.</td>
</tr>
</tbody>
</table>
show ip eigrp neighbors

To display neighbors discovered by the Enhanced Interior Gateway Routing Protocol (EIGRP), use the `show ip eigrp neighbors` command in privileged EXEC mode.

```
show ip eigrp [vrf vrf-name] [autonomous-system-number] neighbors [static | detail] [interface-type interface-number]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Displays information about the specified VPN Routing and Forwarding (VRF) instance.</td>
</tr>
<tr>
<td>autonomous-system-number</td>
<td>(Optional) Autonomous-system-number-specific output is displayed.</td>
</tr>
<tr>
<td>static</td>
<td>(Optional) Displays static neighbors.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed neighbor information.</td>
</tr>
<tr>
<td>interface-type interface-number</td>
<td>(Optional) Interface-specific output is displayed.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show ip eigrp neighbors` command can be used to display information about EIGRP named and EIGRP autonomous-system configurations. Use the `show ip eigrp neighbors` command to display dynamic and static neighbor states. You can use this command for also debugging certain types of transport problems.

This command displays the same information as the `show eigrp address-family neighbors` command. Cisco recommends that you use the `show eigrp address-family neighbors` command.

**Examples**

The following is sample output from the `show ip eigrp neighbors` command:

```
Device#show ip eigrp neighbors

+--------+--------+--------+---------+---------+---------+---------+---------+---------+---------+
| H      | Address | Interface | Hold   | Uptime  | SRTT    | RTO     | Q       | Seq     |
|--------+---------+-----------+--------+---------+---------+---------+---------+---------+
| 0      | 10.1.1.2 | Et0/0     | 13     | 00:00:03| 1996    | 5000    | 0       | 5       |
| 2      | 10.1.1.9 | Et0/0     | 14     | 00:02:24| 206     | 5000    | 0       | 5       |
| 1      | 10.1.2.3 | Et0/1     | 11     | 00:20:39| 2202    | 5000    | 0       | 5       |
```

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

**Table 134: show ip eigrp neighbors Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of the EIGRP peer.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the router is receiving hello packets from the peer.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip eigrp neighbors detail` command:

```
Device#show ip eigrp neighbors detail

EIGRP-IPv4 VR(foo) Address-Family Neighbors for AS(1)
H Address Interface Hold Uptime SRTT RTO Q Seq
   (sec) (ms) Cnt Num
0  192.168.10.1 Gi2/0    12 00:00:21 1600 5000 0 3
  Static neighbor (Lisp Encap)
  Version 8.0/2.0, Retrans: 0, Retries: 0, Prefixes: 1
  Topology-ids from peer - 0
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold</td>
<td>Time in seconds for which EIGRP waits to hear from the peer before declaring it down.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.</td>
</tr>
<tr>
<td>SRTT</td>
<td>Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.</td>
</tr>
<tr>
<td>RTO</td>
<td>Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.</td>
</tr>
<tr>
<td>Q Cnt</td>
<td>Number of EIGRP packets (update, query, and reply) that the software is waiting to send.</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from this neighbor.</td>
</tr>
</tbody>
</table>

**Table 135: show ip eigrp neighbors detail Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.</td>
</tr>
<tr>
<td>Address</td>
<td>IP address of the EIGRP peer.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface on which the router is receiving hello packets from the peer.</td>
</tr>
<tr>
<td>Hold</td>
<td>Time in seconds for which EIGRP waits to hear from the peer before declaring it down.</td>
</tr>
<tr>
<td>Lisp Encap</td>
<td>Indicates that routes from this neighbor are LISP encapsulated.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Elapsed time (in hours:minutes: seconds) since the local router first heard from this neighbor.</td>
</tr>
<tr>
<td>SRTT</td>
<td>Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the local router to receive an acknowledgment of that packet.</td>
</tr>
<tr>
<td>RTO</td>
<td>Retransmission timeout (in milliseconds). This is the amount of time the software waits before resending a packet from the retransmission queue to a neighbor.</td>
</tr>
<tr>
<td>Q Cnt</td>
<td>Number of EIGRP packets (update, query, and reply) that the software is waiting to send.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Seq Num</td>
<td>Sequence number of the last update, query, or reply packet that was received from this neighbor.</td>
</tr>
<tr>
<td>Version</td>
<td>The software version that the specified peer is running.</td>
</tr>
<tr>
<td>Retrans</td>
<td>Number of times that a packet has been retransmitted.</td>
</tr>
<tr>
<td>Retries</td>
<td>Number of times an attempt was made to retransmit a packet.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eigrp address-family neighbors</td>
<td>Displays neighbors discovered by EIGRP.</td>
</tr>
</tbody>
</table>
**show ip eigrp topology**

To display Enhanced Interior Gateway Routing Protocol (EIGRP) topology table entries, use the `show ip eigrp topology` command in user EXEC or privileged EXEC mode.

```
show ip eigrp topology[ [vrf vrf-name] [autonomous-system-number] [network { [mask] } prefix [active] [all-links] [detail-links] [name] [pending] [summary] [zero-successors]]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Displays information about the specified virtual routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>autonomous-system-number</td>
<td>(Optional) Autonomous system number.</td>
</tr>
<tr>
<td>network</td>
<td>(Optional) Network address.</td>
</tr>
<tr>
<td>mask</td>
<td>(Optional) Network mask.</td>
</tr>
<tr>
<td>prefix</td>
<td>(Optional) Network prefix in the format &lt;network&gt;/&lt;length&gt;; for example, 192.168.0.0/16.</td>
</tr>
<tr>
<td>active</td>
<td>(Optional) Displays all topology entries that are in the active state.</td>
</tr>
<tr>
<td>all-links</td>
<td>(Optional) Displays all entries in the EIGRP topology table (including nonfeasible-successor sources).</td>
</tr>
<tr>
<td>detail-links</td>
<td>(Optional) Displays all topology entries with additional details.</td>
</tr>
<tr>
<td>name</td>
<td>(Optional) Displays the IPv4 topology table name. This name is the topology identifier and shows topology-related information for Multitopology Routing (MTR).</td>
</tr>
<tr>
<td>pending</td>
<td>(Optional) Displays all entries in the EIGRP topology table that are either waiting for an update from a neighbor or waiting to reply to a neighbor.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of the EIGRP topology table.</td>
</tr>
<tr>
<td>zero-successors</td>
<td>(Optional) Displays available routes that have zero successors.</td>
</tr>
</tbody>
</table>

**Command Default**

If this command is used without any of the optional keywords, only topology entries with feasible successors are displayed and only feasible paths are shown.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show ip eigrp topology` command to display topology entries, feasible and nonfeasible paths, metrics, and states. This command can be used without any arguments or keywords to display only topology entries.
with feasible successors and feasible paths. The **all-links** keyword displays all paths, whether feasible or not, and the **detail-links** keyword displays additional details about these paths.

Use this command to display information about EIGRP named and EIGRP autonomous system configurations. This command displays the same information as the **show eigrp address-family topology** command. We recommend using the **show eigrp address-family topology** command.

### Examples

The following is sample output from the **show ip eigrp topology** command:

```
Device# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P = Passive, A = Active, U = Update, Q = Query, R = Reply,
       r = Reply status, s = sia status
P 10.0.0.0/8, 1 successors, FD is 409600
   via 192.0.2.1 (409600/128256), Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600
   via 192.0.2.1 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600
   via Summary (281600/0), Null0
P 10.0.1.0/24, 1 successors, FD is 281600
   via Connected, Ethernet0/0
```

The following sample output from the **show ip eigrp topology** **prefix** command displays detailed information about a single prefix. The prefix shown is an EIGRP internal route.

```
Device# show ip eigrp topology 10.0.0.0/8
EIGRP-IPv4 VR(vr1) Topology Entry for AS(1)/ID(10.1.1.2) for 10.0.0.0/8
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 82329600, RIB is 643200
Descriptor Blocks:
10.1.1.1 (Ethernet2/0), from 10.1.1.1, Send flag is 0x0
  Composite metric is (82329600/163840), route is Internal
  Vector metric:
    Minimum bandwidth is 16000 Kbit
    Total delay is 631250000 picoseconds
    Reliability is 255/255
    Load is ½55
    Minimum MTU is 1500
    Hop count is 1
    Originating router is 10.1.1.1
```

The following sample output from the **show ip eigrp topology** **prefix** command displays detailed information about a single prefix. The prefix shown is an EIGRP external route.

```
Device# show ip eigrp topology 172.16.1.0/24
EIGRP-IPv4 Topology Entry for AS(1)/ID(10.0.0.1) for 172.16.1.0/24
State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600, RIB is 643200
Descriptor Blocks:
172.16.1.0/24 (Ethernet0/0), from 10.0.1.2, Send flag is 0x0
  Composite metric is (409600/128256), route is External
  Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 6000 picoseconds
    Reliability is 255/255
    Load is ½55
    Minimum MTU is 1500
    Hop count is 1
```
Originating router is 172.16.1.0/24
External data:
  AS number of route is 0
  External protocol is Connected, external metric is 0
  Administrator tag is 0 (0x00000000)

The following sample output from the `show ip eigrp topology prefix` command displays Equal Cost Multipath (ECMP) mode information when the `no ip next-hop-self` command is configured without the `no-ecmp-mode` keyword in an EIGRP topology. The ECMP mode provides information about the path that is being advertised. If there is more than one successor, the top most path will be advertised as the default path over all interfaces, and “ECMP Mode: Advertise by default” will be displayed in the output. If any path other than the default path is advertised, “ECMP Mode: Advertise out <Interface name>” will be displayed.

The topology table displays entries of routes for a particular prefix. The routes are sorted based on metric, next-hop, and infosource. In a Dynamic Multipoint VPN (DMVPN) scenario, routes with same metric and next-hop are sorted based on infosource. The top route in the ECMP is always advertised.

Device# show ip eigrp topology 192.168.10.0/24

EIGRP-IPv4 Topology Entry for AS(1)/ID(10.10.100.100) for 192.168.10.0/24
State is Passive, Query origin flag is 1, 2 Successor(s), FD is 284160
Descriptor Blocks:
  10.100.1.0 (Tunnel0), from 10.100.0.1, Send flag is 0x0
    Composite metric is (284160/281600), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 1100 microseconds
      Reliability is 255/255
      Load is 4/5
      Minimum MTU is 1400
      Hop count is 1
      Originating router is 10.10.1.1
      ECMP Mode: Advertise by default
  10.100.0.2 (Tunnel1), from 10.100.0.2, Send flag is 0x0
    Composite metric is (284160/281600), route is Internal
    Vector metric:
      Minimum bandwidth is 10000 Kbit
      Total delay is 1100 microseconds
      Reliability is 255/255
      Load is 4/5
      Minimum MTU is 1400
      Hop count is 1
      Originating router is 10.10.2.2
      ECMP Mode: Advertise out Tunnel1

The following sample output from the `show ip eigrp topology all-links` command displays all paths, even those that are not feasible:

Device# show ip eigrp topology all-links

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
   via 10.10.1.2 (409600/128256), Ethernet0/0
   via 10.1.4.3 (2586111744/2585599744), Serial3/0, serno 18

The following sample output from the `show ip eigrp topology detail-links` command displays additional details about routes:
Device#`show ip eigrp topology detail-links`

EIGRP-IPv4 Topology Table for AS(1)/ID(10.0.0.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
      r - reply Status, s - sia Status

P 10.0.0.0/8, 1 successors, FD is 409600, serno 6
  via 10.10.1.2 (409600/128256), Ethernet0/0
P 172.16.1.0/24, 1 successors, FD is 409600, serno 14
  via 10.10.1.2 (409600/128256), Ethernet0/0
P 10.0.0.0/8, 1 successors, FD is 281600, serno 3
  via Summary (281600/0), Null0
P 10.1.1.0/24, 1 successors, FD is 281600, serno 1
  via Connected, Ethernet0/0

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

Table 136: `show ip eigrp topology` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Codes</td>
<td>State of this topology table entry. Passive and Active refer to the EIGRP state with respect to the destination. Update, Query, and Reply refer to the type of packet that is being sent.</td>
</tr>
<tr>
<td></td>
<td>• P - Passive—Indicates that no EIGRP computations are being performed for this route.</td>
</tr>
<tr>
<td></td>
<td>• A - Active—Indicates that EIGRP computations are being performed for this route.</td>
</tr>
<tr>
<td></td>
<td>• U - Update—Indicates that a pending update packet is waiting to be sent for this route.</td>
</tr>
<tr>
<td></td>
<td>• Q - Query—Indicates that a pending query packet is waiting to be sent for this route.</td>
</tr>
<tr>
<td></td>
<td>• R - Reply—Indicates that a pending reply packet is waiting to be sent for this route.</td>
</tr>
<tr>
<td></td>
<td>• r - Reply status—Indicates that EIGRP has sent a query for the route and is waiting for a reply from the specified path.</td>
</tr>
<tr>
<td></td>
<td>• s - sia status—Indicates that the EIGRP query packet is in stuck-in-active (SIA) status.</td>
</tr>
<tr>
<td>successors</td>
<td>Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or the next hop is in a transition state.</td>
</tr>
<tr>
<td>serno</td>
<td>Serial number.</td>
</tr>
</tbody>
</table>
Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route became active. This value is used in the feasibility condition check. If the reported distance of the device is less than the feasible distance, the feasibility condition is met and that route becomes a feasible successor. After the software determines that it has a feasible successor, the software need not send a query for that destination.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FD</td>
<td>Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route became active. This value is used in the feasibility condition check. If the reported distance of the device is less than the feasible distance, the feasibility condition is met and that route becomes a feasible successor. After the software determines that it has a feasible successor, the software need not send a query for that destination.</td>
</tr>
<tr>
<td>via</td>
<td>Next-hop address that advertises the passive route.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eigrp address-family topology</td>
<td>Displays entries in the EIGRP address-family topology table.</td>
</tr>
</tbody>
</table>
show ip eigrp traffic

To display the number of Enhanced Interior Gateway Routing Protocol (EIGRP) packets sent and received, use the `show ip eigrp traffic` command in privileged EXEC mode.

```
show ip eigrp [vrf {vrf-name | *}] [autonomous-system-number] traffic
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Displays information about the specified VRF.</td>
</tr>
<tr>
<td><code>vrf *</code></td>
<td>(Optional) Displays information about all VRFs.</td>
</tr>
<tr>
<td><code>autonomous-system-number</code></td>
<td>(Optional) Autonomous system number.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command can be used to display information about EIGRP named configurations and EIGRP autonomous-system (AS) configurations.

This command displays the same information as the `show eigrp address-family traffic` command. Cisco recommends using the `show eigrp address-family traffic` command.

**Examples**

The following is sample output from the `show ip eigrp traffic` command:

```
Device# show ip eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS(60)
Hellos sent/received: 21429/2809
Updates sent/received: 22/17
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 16/13
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
Hello Process ID: 204
PDM Process ID: 203
Socket Queue: 0/2000/2/0 (current/max/highest/drops)
Input Queue: 0/2000/2/0 (current/max/highest/drops)
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hellos sent/received</td>
<td>Number of hello packets sent and received.</td>
</tr>
<tr>
<td>Updates sent/received</td>
<td>Number of update packets sent and received.</td>
</tr>
<tr>
<td>Queries sent/received</td>
<td>Number of query packets sent and received.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replies sent/received</td>
<td>Number of reply packets sent and received.</td>
</tr>
<tr>
<td>Acks sent/received</td>
<td>Number of acknowledgement packets sent and received.</td>
</tr>
<tr>
<td>SIA-Queries sent/received</td>
<td>Number of stuck in active query packets sent and received.</td>
</tr>
<tr>
<td>SIA-Replies sent/received</td>
<td>Number of stuck in active reply packets sent and received.</td>
</tr>
<tr>
<td>Hello Process ID</td>
<td>Hello process identifier.</td>
</tr>
<tr>
<td>Socket Queue</td>
<td>The IP to EIGRP Hello Process socket queue counters.</td>
</tr>
<tr>
<td>Input queue</td>
<td>The EIGRP Hello Process to EIGRP PDM socket queue counters.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show eigrp address-family traffic</td>
<td>Displays the number of EIGRP packets sent and received.</td>
</tr>
</tbody>
</table>
show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the `show ip ospf` command in user EXEC or privileged EXEC mode.

```
show ip ospf [process-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Process ID. If this argument is included, only information for the specified routing process is included.</td>
</tr>
</tbody>
</table>

**Command Modes**

- User EXEC
- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Mainline Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ip ospf` command when entered without a specific OSPF process ID:

```
Device# show ip ospf

Routing Process "ospf 201" with ID 10.0.0.1 and Domain ID 10.20.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPF 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
LSA group pacing timer 100 secs
Interface flood pacing timer 55 msecs
Retransmission pacing timer 100 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 2. 2 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE (0)
  Number of interfaces in this area is 2
  Area has message digest authentication
  SPF algorithm executed 4 times
  Area ranges are
  Number of LSA 4. Checksum Sum 0x29BEB
  Number of opaque link LSA 0. Checksum Sum 0x0
  Number of DCbitless LSA 3
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
Area 172.16.26.0
  Number of interfaces in this area is 0
  Area has no authentication
  SPF algorithm executed 1 times
  Area ranges are
  192.168.0.0/16 Passive Advertise
  Number of LSA 1. Checksum Sum 0x44FD
  Number of opaque link LSA 0. Checksum Sum 0x0
  Number of DCbitless LSA 1
```
Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the `show ip ospf` command to verify that the BFD feature has been enabled for OSPF process 123. The relevant command output is shown in bold in the output.

```
Device# show ip ospf
Routing Process "ospf 123" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of external LSA 0. Checksum Sum 0x000000
Number of area in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  BFD is enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 00:00:03.708 ago
    SPF algorithm executed 27 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x00AEF1
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

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

**Table 138: show ip ospf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process “ospf 201”</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports...</td>
<td>Number of types of service supported (Type 0 only).</td>
</tr>
<tr>
<td>SPF schedule delay</td>
<td>Delay time (in seconds) of SPF calculations.</td>
</tr>
<tr>
<td>Minimum LSA interval</td>
<td>Minimum interval (in seconds) between link-state advertisements.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LSA group pacing timer</td>
<td>Configured LSA group pacing timer (in seconds).</td>
</tr>
<tr>
<td>Interface flood pacing timer</td>
<td>Configured LSA flood pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Retransmission pacing timer</td>
<td>Configured LSA retransmission pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Number of external LSA</td>
<td>Number of external link-state advertisements.</td>
</tr>
<tr>
<td>Number of opaque AS LSA</td>
<td>Number of opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of DCbitless external and opaque AS LSA</td>
<td>Number of demand circuit external and opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of DoNotAge external and opaque AS LSA</td>
<td>Number of do not age external and opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of areas in this router is</td>
<td>Number of areas configured for the router.</td>
</tr>
<tr>
<td>External flood list length</td>
<td>External flood list length.</td>
</tr>
<tr>
<td>BFD is enabled</td>
<td>BFD has been enabled on the OSPF process.</td>
</tr>
</tbody>
</table>

The following is an excerpt of output from the `show ip ospf` command when the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured:

```
Device#show ip ospf
.
.
Area 2
    Number of interfaces in this area is 4
    It is a NSSA area
    Perform type-7/type-5 LSA translation, suppress forwarding address
.
.
Routing Process "ospf 1" with ID 192.168.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPF's 10000 msecs
  Maximum wait time between two consecutive SPF's 10000 msecs
  Incremental-SPF disabled
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  Number of external LSA 0. Checksum Sum 0x0
  Number of opaque AS LSA 0. Checksum Sum 0x0
  Number of DCbitless external and opaque AS LSA 0
  Number of DoNotAge external and opaque AS LSA 0
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  External flood list length 0
```
The table below describes the significant fields shown in the display.

**Table 139: show ip ospf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>OSPF area and tag.</td>
</tr>
<tr>
<td>Number of interfaces...</td>
<td>Number of interfaces configured in the area.</td>
</tr>
<tr>
<td>It is...</td>
<td>Possible types are internal, area border, or autonomous system boundary.</td>
</tr>
<tr>
<td>Routing process “ospf 1” with ID 192.168.0.1</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports...</td>
<td>Number of types of service supported (Type 0 only).</td>
</tr>
<tr>
<td>Initial SPF schedule delay</td>
<td>Delay time of SPF calculations at startup.</td>
</tr>
<tr>
<td>Minimum hold time</td>
<td>Minimum hold time (in milliseconds) between consecutive SPF calculations.</td>
</tr>
<tr>
<td>Maximum wait time</td>
<td>Maximum wait time (in milliseconds) between consecutive SPF calculations.</td>
</tr>
<tr>
<td>Incremental-SPF</td>
<td>Status of incremental SPF calculations.</td>
</tr>
<tr>
<td>Minimum LSA...</td>
<td>Minimum time interval (in seconds) between link-state advertisements, and minimum arrival time (in milliseconds) of link-state advertisements,</td>
</tr>
<tr>
<td>LSA group pacing timer</td>
<td>Configured LSA group pacing timer (in seconds).</td>
</tr>
<tr>
<td>Interface flood pacing timer</td>
<td>Configured LSA flood pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Retransmission pacing timer</td>
<td>Configured LSA retransmission pacing timer (in milliseconds).</td>
</tr>
<tr>
<td>Number of...</td>
<td>Number and type of link-state advertisements that have been received.</td>
</tr>
<tr>
<td>Number of external LSA</td>
<td>Number of external link-state advertisements.</td>
</tr>
<tr>
<td>Number of opaque AS LSA</td>
<td>Number of opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of DC bitless external and opaque AS LSA</td>
<td>Number of demand circuit external and opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of DoNotAge external and opaque AS LSA</td>
<td>Number of do not age external and opaque link-state advertisements.</td>
</tr>
<tr>
<td>Number of areas in this router is</td>
<td>Number of areas configured for the router listed by type.</td>
</tr>
<tr>
<td>External flood list length</td>
<td>External flood list length.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip ospf` command. In this example, the user had configured the `redistribution maximum-prefix` command to set a limit of 2000 redistributed routes. SPF throttling was configured with the `timer throttlespf` command.

```
Device# show ip ospf 1
Routing Process "ospf 1" with ID 10.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process “ospf 1” with ID 10.0.0.1</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports ...</td>
<td>Number of Types of Service supported.</td>
</tr>
<tr>
<td>It is ...</td>
<td>Possible types are internal, area border, or autonomous system boundary router.</td>
</tr>
<tr>
<td>Redistributing External Routes from</td>
<td>Lists of redistributed routes, by protocol.</td>
</tr>
<tr>
<td>Maximum limit of redistributed prefixes</td>
<td>Value set in the <code>redistribution maximum-prefix</code> command to set a limit on the number of redistributed routes.</td>
</tr>
<tr>
<td>Threshold for warning message</td>
<td>Percentage set in the <code>redistribution maximum-prefix</code> command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.</td>
</tr>
<tr>
<td>Initial SPF schedule delay</td>
<td>Delay (in milliseconds) before initial SPF schedule for SPF throttling. Configured with the <code>timer throttlespf</code> command.</td>
</tr>
<tr>
<td>Minimum hold time between two consecutive SPFs</td>
<td>Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <code>timer throttlespf</code> command.</td>
</tr>
<tr>
<td>Maximum wait time between two consecutive SPFs</td>
<td>Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <code>timer throttlespf</code> command.</td>
</tr>
<tr>
<td>Number of areas</td>
<td>Number of areas in router, area addresses, and so on.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip ospf` command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.
Device#show ip ospf 1
Routing Process "ospf 4" with ID 10.10.24.4
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Initial LSA throttle delay 100 msecs
Minimum hold time for LSA throttle 10000 msecs
Maximum wait time for LSA throttle 45000 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area 24
  Number of interfaces in this area is 2
  Area has no authentication
  SPF algorithm last executed 04:28:18.396 ago
  SPF algorithm executed 8 times
Area ranges are
  Number of LSA 4. Checksum Sum 0x23EB9
  Number of opaque link LSA 0. Checksum Sum 0x0
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0

The following is sample show ip ospf command. In this example, the user had configured the redistribution maximum-prefix command to set a limit of 2000 redistributed routes. SPF throttling was configured with the timer throttle spf command.

Device#show ip ospf 1
Routing Process "ospf 1" with ID 192.168.0.0
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from
static, includes subnets in redistribution
  Maximum limit of redistributed prefixes 2000
  Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs

The table below describes the significant fields shown in the display.
Table 141: show ip ospf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing process “ospf 1” with ID 192.168.0.0.</td>
<td>Process ID and OSPF router ID.</td>
</tr>
<tr>
<td>Supports ...</td>
<td>Number of TOS supported.</td>
</tr>
<tr>
<td>It is ...</td>
<td>Possible types are internal, area border, or autonomous system boundary routers.</td>
</tr>
<tr>
<td>Redistributing External Routes from</td>
<td>Lists of redistributed routes, by protocol.</td>
</tr>
<tr>
<td>Maximum limit of redistributed prefixes</td>
<td>Value set in the \texttt{redistributionmaximum-prefix} command to set a limit on the number of redistributed routes.</td>
</tr>
<tr>
<td>Threshold for warning message</td>
<td>Percentage set in the \texttt{redistributionmaximum-prefix} command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.</td>
</tr>
<tr>
<td>Initial SPF schedule delay</td>
<td>Delay (in milliseconds) before the initial SPF schedule for SPF throttling. Configured with the \texttt{timerthrottlespf} command.</td>
</tr>
<tr>
<td>Minimum hold time between two consecutive SPFs</td>
<td>Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the \texttt{timerthrottlespf} command.</td>
</tr>
<tr>
<td>Maximum wait time between two consecutive SPFs</td>
<td>Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the \texttt{timerthrottlespf} command.</td>
</tr>
<tr>
<td>Number of areas</td>
<td>Number of areas in router, area addresses, and so on.</td>
</tr>
</tbody>
</table>

The following is sample output from the \texttt{show ip ospf} command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Device#show ip ospf 1
Routing Process "ospf 4" with ID 10.10.24.4
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Incremental-SPF disabled
Initial LSA throttle delay 100 msecs
Minimum hold time for LSA throttle 10000 msecs
Maximum wait time for LSA throttle 45000 msecs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa

External flood list length 0

Area 24

Number of interfaces in this area is 2
Area has no authentication
SPF algorithm last executed 04:28:18.396 ago
SPF algorithm executed 8 times
Area ranges are
Number of LSA 4. Checksum Sum 0x23EB9
Number of opaque link LSA 0. Checksum Sum 0x0
Number of DCbitless LSA 0
Number of indication LSA 0
Number of DoNotAge LSA 0
Flood list length 0
**show ip ospf border-routers**

To display the internal Open Shortest Path First (OSPF) routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR), use the `show ip ospf border-routers` command in privileged EXEC mode.

**show ip ospf border-routers**

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ip ospf border-routers` command:

```
Device# show ip ospf border-routers
OSPF Process 109 Internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 192.168.97.53 [10] via 172.16.1.53, Serial0, ABR, Area 0.0.0.3, SPF 3
i 192.168.103.51 [10] via 192.168.96.51, Serial0, ABR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 192.168.96.51, Serial0, ASBR, Area 0.0.0.3, SPF 3
I 192.168.103.52 [22] via 172.16.1.53, Serial0, ASBR, Area 0.0.0.3, SPF 3
```

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

**Table 142: show ip ospf border-routers Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.97.53</td>
<td>Router ID of the destination.</td>
</tr>
<tr>
<td>[10]</td>
<td>Cost of using this route.</td>
</tr>
<tr>
<td>via 172.16.1.53</td>
<td>Next hop toward the destination.</td>
</tr>
<tr>
<td>Serial0</td>
<td>Interface type for the outgoing interface.</td>
</tr>
<tr>
<td>ABR</td>
<td>The router type of the destination; it is either an ABR or ASBR or both.</td>
</tr>
<tr>
<td>Area</td>
<td>The area ID of the area from which this route is learned.</td>
</tr>
<tr>
<td>SPF 3</td>
<td>The internal number of the shortest path first (SPF) calculation that installs this route.</td>
</tr>
</tbody>
</table>
**show ip ospf database**

To display lists of information related to the Open Shortest Path First (OSPF) database for a specific router, use the `show ip ospf database` command in EXEC mode.

```plaintext
show ip ospf [process-id area-id] database
show ip ospf [process-id area-id] database [adv-router [ip-address]]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [asbr-summary] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [database-summary]
show ip ospf [process-id database] [external] [link-state-id]
show ip ospf [process-id database] [external] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [external] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [network] [link-state-id]
show ip ospf [process-id area-id] database [network] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [network] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [nssa-external] [link-state-id] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [router] [link-state-id]
show ip ospf [process-id area-id] database [router] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [router] [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [self-originate] [link-state-id]
show ip ospf [process-id area-id] database [summary] [link-state-id]
show ip ospf [process-id area-id] database [summary] [link-state-id] [adv-router [ip-address]]
show ip ospf [process-id area-id] database [summary] [link-state-id] [self-originate] [link-state-id]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Internal identification. It is locally assigned and can be any positive integer. The number used here is the number assigned administratively when enabling the OSPF routing process.</td>
</tr>
<tr>
<td>area-id</td>
<td>(Optional) Area number associated with the OSPF address range defined in the <code>network</code> router configuration command used to define the particular area.</td>
</tr>
<tr>
<td>adv-router [ip-address]</td>
<td>(Optional) Displays all the LSAs of the specified router. If no IP address is included, the information is about the local router itself (in this case, the same as self-originate).</td>
</tr>
</tbody>
</table>
**link-state-id**
(Optional) Portion of the Internet environment that is being described by the advertisement. The value entered depends on the advertisement’s LS type. It must be entered in the form of an IP address.

When the link state advertisement is describing a network, the *link-state-id* can take one of two forms:
- The network’s IP address (as in type 3 summary link advertisements and in autonomous system external link advertisements).
- A derived address obtained from the link state ID. (Note that masking a network links advertisement’s link state ID with the network’s subnet mask yields the network’s IP address.)

When the link state advertisement is describing a router, the link state ID is always the described router’s OSPF router ID.

When an autonomous system external advertisement (LS Type = 5) is describing a default route, its link state ID is set to Default Destination (0.0.0.0).

**asbr-summary**
(Optional) Displays information only about the autonomous system boundary router summary LSAs.

**database-summary**
(Optional) Displays how many of each type of LSA for each area there are in the database, and the total.

**external**
(Optional) Displays information only about the external LSAs.

**network**
(Optional) Displays information only about the network LSAs.

**nssa-external**
(Optional) Displays information only about the NSSA external LSAs.

**router**
(Optional) Displays information only about the router LSAs.

**self originate**
(Optional) Displays only self-originated LSAs (from the local router).

**summary**
(Optional) Displays information only about the summary LSAs.

---

**Command Modes**

**EXEC**

---

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

The various forms of this command deliver information about different OSPF link state advertisements.

---

**Examples**

The following is sample output from the `show ip ospf database` command when no arguments or keywords are used:

```
Device#show ip ospf database
OSPF Router with Id(192.168.239.66) (Process ID 300)
    Displaying Router Link States(Area 0.0.0.0)
        Link ID        ADV Router   Age   Seq#        Checksum  Link count
        172.16.21.6    172.16.21.6  1731  0x80002CFB  0x69BC       8
```
<table>
<thead>
<tr>
<th>Link ID</th>
<th>ADV Router</th>
<th>Age</th>
<th>Seq#</th>
<th>Checksum</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.21.5</td>
<td>172.16.21.5</td>
<td>1112</td>
<td>0x800009D2</td>
<td>0xA2B8</td>
</tr>
<tr>
<td>172.16.1.2</td>
<td>172.16.1.2</td>
<td>1662</td>
<td>0x80000A98</td>
<td>0x4CB6</td>
</tr>
<tr>
<td>172.16.1.1</td>
<td>172.16.1.1</td>
<td>1115</td>
<td>0x800009B6</td>
<td>0x5F2C</td>
</tr>
<tr>
<td>172.16.1.5</td>
<td>172.16.1.5</td>
<td>1691</td>
<td>0x80002BC</td>
<td>0x2A1A</td>
</tr>
<tr>
<td>172.16.65.6</td>
<td>172.16.65.6</td>
<td>1395</td>
<td>0x80001947</td>
<td>0xEEE1</td>
</tr>
<tr>
<td>172.16.241.5</td>
<td>172.16.241.5</td>
<td>1161</td>
<td>0x8000007C</td>
<td>0x7C70</td>
</tr>
<tr>
<td>172.16.27.6</td>
<td>172.16.27.6</td>
<td>1723</td>
<td>0x80000548</td>
<td>0x8641</td>
</tr>
<tr>
<td>172.16.70.6</td>
<td>172.16.70.6</td>
<td>1485</td>
<td>0x80000B97</td>
<td>0xEBB4</td>
</tr>
</tbody>
</table>

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

**Table 143: show ip ospf Database Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link ID</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>ADV Router</td>
<td>Advertising router’s ID.</td>
</tr>
<tr>
<td>Age</td>
<td>Link state age.</td>
</tr>
<tr>
<td>Seq#</td>
<td>Link state sequence number (detects old or duplicate link state advertisements).</td>
</tr>
<tr>
<td>Checksum</td>
<td>Fletcher checksum of the complete contents of the link state advertisement.</td>
</tr>
<tr>
<td>Link count</td>
<td>Number of interfaces detected for router.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip ospf database` command with the `asbr-summary` keyword:

```
Device# show ip ospf database asbr-summary
OSPF Router with id (192.168.239.66) (Process ID 300)
  Displaying Summary ASB Link States (Area 0.0.0.0)
    LS age: 1463
    Options: (No TOS-capability)
    LS Type: Summary Links (AS Boundary Router)
    Link State ID: 172.16.245.1 (AS Boundary Router address)
    Advertising Router: 172.16.241.5
    LS Seq Number: 80000072
    Checksum: 0x3548
    Length: 28
    Network Mask: 0.0.0.0 TOS: 0 Metric: 1
```

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

**Table 144: show ip ospf database asbr-summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip ospf database` command with the `external` keyword:

```
Device#show ip ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
            Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.105.0.0 (External Network Number)
Advertising Router: 172.16.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 1
    Forward Address: 0.0.0.0
    External Route Tag: 0
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Autonomous system</td>
<td>OSPF autonomous system number (OSPF process ID).</td>
</tr>
<tr>
<td>LS age</td>
<td>Link state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
</tbody>
</table>
### Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LS Type</td>
<td>Link state type.</td>
</tr>
<tr>
<td>Link State ID</td>
<td>Link state ID (external network number).</td>
</tr>
<tr>
<td>Advertising Router</td>
<td>Advertising router’s ID.</td>
</tr>
<tr>
<td>LS Seq Number</td>
<td>Link state sequence number (detects old or duplicate link state advertisements).</td>
</tr>
<tr>
<td>Checksum</td>
<td>LS checksum (Fletcher checksum of the complete contents of the LSA).</td>
</tr>
<tr>
<td>Length</td>
<td>Length in bytes of the link state advertisement.</td>
</tr>
<tr>
<td>Network Mask</td>
<td>Network mask implemented.</td>
</tr>
<tr>
<td>Metric Type</td>
<td>External Type.</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of service.</td>
</tr>
<tr>
<td>Metric</td>
<td>Link state metric.</td>
</tr>
<tr>
<td>Forward Address</td>
<td>Forwarding address. Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded instead to the advertisement’s originator.</td>
</tr>
<tr>
<td>External Route Tag</td>
<td>External route tag, a 32-bit field attached to each external route. This is not used by the OSPF protocol itself.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip ospf database` command with the `network` keyword:

```
Device#show ip ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
    Displaying Net Link States(Area 0.0.0.0)
    LS age: 1367
    Options: (No TOS-capability)
    LS Type: Network Links
    Link State ID: 172.16.1.3 (address of Designated Router)
    Advertising Router: 192.168.239.66
    LS Seq Number: 800000E7
    Checksum: 0x1229
    Length: 52
    Network Mask: 255.255.255.0
    Attached Router: 192.168.239.66
    Attached Router: 172.16.241.5
    Attached Router: 172.16.1.1
    Attached Router: 172.16.54.5
    Attached Router: 172.16.1.5
```

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

### Table 146: show ip ospf database network Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID 300</td>
<td>OSPF process ID.</td>
</tr>
</tbody>
</table>
The following is sample output from the `show ip ospf database` command with the `router` keyword:

```
Device#show ip ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Router Link States (Area 0.0.0.0)
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 172.16.21.6
Advertising Router: 172.16.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
155 Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 172.16.21.5
(Link Data) Router Interface address: 172.16.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

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

### Table 147: show ip ospf database router Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router with id</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link state age.</td>
</tr>
</tbody>
</table>

---
The following is sample output from `show ip ospf database` command with the `summary` keyword:

```
Device# show ip ospf database summary
  OSPF Router with id(192.168.239.66) (Process ID 300)
    Displaying Summary Net Link States (Area 0.0.0.0)
  LS age: 1401
  Options: (No TOS-capability)
  LS Type: Summary Links (Network)
  Link State ID: 172.16.240.0 (summary Network Number)
  Advertising Router: 172.16.241.5
  LS Seq Number: 80000072
  Checksum: 0x84FF
  Length: 28
  Network Mask: 255.255.255.0  TOS: 0  Metric: 1
```

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

```
Table 148: show ip ospf database summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSPF Router</td>
<td>Router ID number.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>LS age</td>
<td>Link state age.</td>
</tr>
<tr>
<td>Options</td>
<td>Type of service options (Type 0 only).</td>
</tr>
<tr>
<td>LS Type</td>
<td>Link state type.</td>
</tr>
</tbody>
</table>
The following is sample output from `show ip ospf database database-summary` command with the `database-summary` keyword:

```
Device# show ip ospf database database-summary
OSPF Router with ID (10.0.0.1) (Process ID 1)
Area 0 database summary
    LSA Type  Count  Delete  Maxage
    Router    3      0       0
    Network   0      0       0
    Summary Net  0     0       0
    Summary ASBR 0     0       0
    Type-7 Ext 0      0       0
    Self-originated Type-7 0
    Opaque Link 0     0       0
    Opaque Area 0     0       0
Subtotal 3 0 0
Process 1 database summary
    LSA Type  Count  Delete  Maxage
    Router   300     0       0
    Network  0      0       0
    Summary Net  0    0       0
    Summary ASBR 0    0       0
    Type-7 Ext 0    0       0
    Opaque Link 0    0       0
    Opaque Area 0    0       0
    Type-5 Ext 0    0       0
    Self-originated Type-5 200
Opaque AS 0 0 0
Total 203 0 0
```

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

### Table 149: show ip ospf database database-summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area 0 database summary</td>
<td>Area number.</td>
</tr>
<tr>
<td>Count</td>
<td>Count of LSAs of the type identified in the first column.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Router</td>
<td>Number of router link state advertisements in that area.</td>
</tr>
<tr>
<td>Network</td>
<td>Number of network link state advertisements in that area.</td>
</tr>
<tr>
<td>Summary Net</td>
<td>Number of summary link state advertisements in that area.</td>
</tr>
<tr>
<td>Summary ASBR</td>
<td>Number of summary autonomous system boundary router (ASBR) link state advertisements in that area.</td>
</tr>
<tr>
<td>Type-7 Ext</td>
<td>Type-7 LSA count.</td>
</tr>
<tr>
<td>Self-originated Type-7</td>
<td>Self-originated Type-7 LSA.</td>
</tr>
<tr>
<td>Opaque Link</td>
<td>Type-9 LSA count.</td>
</tr>
<tr>
<td>Opaque Area</td>
<td>Type-10 LSA count</td>
</tr>
<tr>
<td>Subtotal</td>
<td>Sum of LSAs for that area.</td>
</tr>
<tr>
<td>Delete</td>
<td>Number of link state advertisements that are marked “Deleted” in that area.</td>
</tr>
<tr>
<td>Maxage</td>
<td>Number of link state advertisements that are marked “Maxaged” in that area.</td>
</tr>
<tr>
<td>Process 1 database summary</td>
<td>Database summary for the process.</td>
</tr>
<tr>
<td>Count</td>
<td>Count of LSAs of the type identified in the first column.</td>
</tr>
<tr>
<td>Router</td>
<td>Number of router link state advertisements in that process.</td>
</tr>
<tr>
<td>Network</td>
<td>Number of network link state advertisements in that process.</td>
</tr>
<tr>
<td>Summary Net</td>
<td>Number of summary link state advertisements in that process.</td>
</tr>
<tr>
<td>Summary ASBR</td>
<td>Number of summary autonomous system boundary router (ASBR) link state advertisements in that process.</td>
</tr>
<tr>
<td>Type-7 Ext</td>
<td>Type-7 LSA count.</td>
</tr>
<tr>
<td>Opaque Link</td>
<td>Type-9 LSA count.</td>
</tr>
<tr>
<td>Opaque Area</td>
<td>Type-10 LSA count</td>
</tr>
<tr>
<td>Type-5 Ext</td>
<td>Type-5 LSA count.</td>
</tr>
<tr>
<td>Self-Originated Type-5</td>
<td>Self-originated Type-5 LSA count.</td>
</tr>
<tr>
<td>Opaque AS</td>
<td>Type-11 LSA count.</td>
</tr>
<tr>
<td>Total</td>
<td>Sum of LSAs for that process.</td>
</tr>
<tr>
<td>Delete</td>
<td>Number of link state advertisements that are marked “Deleted” in that process.</td>
</tr>
<tr>
<td>Maxage</td>
<td>Number of link state advertisements that are marked “Maxaged” in that process.</td>
</tr>
</tbody>
</table>
show ip ospf interface

To display interface information related to Open Shortest Path First (OSPF), use the `show ip ospf interface` command in user EXEC or privileged EXEC mode.

**show ip [ospf] [process-id] interface [type number] [brief] [multicast] [topology {topology-name | base}]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>process-id</td>
<td>(Optional) Process ID number. If this argument is included, only information for the specified routing process is included. The range is 1 to 65535.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. If the <code>type</code> argument is included, only information for the specified interface type is included.</td>
</tr>
<tr>
<td>number</td>
<td>(Optional) Interface number. If the <code>number</code> argument is included, only information for the specified interface number is included.</td>
</tr>
<tr>
<td>brief</td>
<td>(Optional) Displays brief overview information for OSPF interfaces, states, addresses and masks, and areas on the device.</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Displays multicast information.</td>
</tr>
<tr>
<td>topology topology-name</td>
<td>(Optional) Displays OSPF-related information about the named topology instance.</td>
</tr>
<tr>
<td>topology base</td>
<td>(Optional) Displays OSPF-related information about the base topology.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show ip ospf interface` command when Ethernet interface 0/0 is specified:

```
Device#show ip ospf interface ethernet 0/0

Ethernet0/0 is up, line protocol is up
  Internet Address 192.168.254.202/24, Area 0
  Process ID 1, Router ID 192.168.99.1, Network Type BROADCAST, Cost: 10
  Topology-MTID Cost Disabled Shutdown Topology Name
  0 10 no no Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.99.1, Interface address 192.168.254.202
  Backup Designated router (ID) 192.168.254.10, Interface address 192.168.254.10
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:05
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
```
In Cisco IOS Release 12.2(33)SRB, the following sample output from the `show ip ospf interface brief topology VOICE` command shows a summary of information, including a confirmation that the Multitopology Routing (MTR) VOICE topology is configured in the interface configuration:

```
Device# show ip ospf interface brief topology VOICE

VOICE Topology (MTID 10)
Interface    PID  Area    IP Address/Mask  Cost  State  Nbrs  F/C
Lo0          1     0      10.0.0.2/32     1     LOOP  0/0
Se2/0        1     0      10.1.0.2/30    10    P2P    1/1
```

The following sample output from the `show ip ospf interface brief topology VOICE` command displays details of the MTR VOICE topology for the interface. When the command is entered without the `brief` keyword, more information is displayed.

```
Device# show ip ospf interface topology VOICE

VOICE Topology (MTID 10)
Loopback0 is up, line protocol is up
Internet Address 10.0.0.2/32, Area 0
Process ID 1, Router ID 10.0.0.2, Network Type LOOPBACK
Topology-MTID  Cost  Disabled  Shutdown  Topology Name
       10    1     no        no      VOICE
Loopback interface is treated as a stub Host Serial2/0 is up, line protocol is up
Internet Address 10.1.0.2/30, Area 0
Process ID 1, Router ID 10.0.0.2, Network Type POINT_TO_POINT
Topology-MTID  Cost  Disabled  Shutdown  Topology Name
       10    10    no        no      VOICE
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:03
Supports Link-local Signaling (LLS)
Cisco NSF helper support enabled
IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.0.0.1
Suppress hello for 0 neighbor(s)
```

In Cisco IOS Release 12.2(33)SRC, the following sample output from the `show ip ospf interface` command displays details about the configured Time-to-Live (TTL) limits:

```
Device# show ip ospf interface ethernet 0

Strict TTL checking enabled
! or a message similar to the following is displayed
Strict TTL checking enabled, up to 4 hops allowed
```

IETF NSF helper support enabled
Index 1/1, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 192.168.254.10 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
The table below describes the significant fields shown in the displays.

**Table 150: show ip ospf interface Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Status of the physical link and operational status of the protocol.</td>
</tr>
<tr>
<td>Process ID</td>
<td>OSPF process ID.</td>
</tr>
<tr>
<td>Area</td>
<td>OSPF area.</td>
</tr>
<tr>
<td>Cost</td>
<td>Administrative cost assigned to the interface.</td>
</tr>
<tr>
<td>State</td>
<td>Operational state of the interface.</td>
</tr>
<tr>
<td>Nbrs F/C</td>
<td>OSPF neighbor count.</td>
</tr>
<tr>
<td>Internet Address</td>
<td>Interface IP address, subnet mask, and area address.</td>
</tr>
<tr>
<td>Topology-MTID</td>
<td>MTR topology Multitopology Identifier (MTID). A number assigned so that the protocol can identify the topology associated with information that it sends to its peers.</td>
</tr>
<tr>
<td>Transmit Delay</td>
<td>Transmit delay in seconds, interface state, and device priority.</td>
</tr>
<tr>
<td>Designated Router</td>
<td>Designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Backup Designated router</td>
<td>Backup designated router ID and respective interface IP address.</td>
</tr>
<tr>
<td>Timer intervals configured</td>
<td>Configuration of timer intervals.</td>
</tr>
<tr>
<td>Hello</td>
<td>Number of seconds until the next hello packet is sent out this interface.</td>
</tr>
<tr>
<td>Strict TTL checking enabled</td>
<td>Only one hop is allowed.</td>
</tr>
<tr>
<td>Strict TTL checking enabled, up to 4 hops allowed</td>
<td>A set number of hops has been explicitly configured.</td>
</tr>
<tr>
<td>Neighbor Count</td>
<td>Count of network neighbors and list of adjacent neighbors.</td>
</tr>
</tbody>
</table>
show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the show ip ospf neighbor command in privileged EXEC mode.

**show ip ospf neighbor [interface-type interface-number] [neighbor-id] [detail] [summary [per-instance]]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-type</td>
<td>(Optional) Type and number associated with a specific OSPF interface.</td>
</tr>
<tr>
<td>interface-number</td>
<td>(Optional) Type and number associated with a specific OSPF interface.</td>
</tr>
<tr>
<td>neighbor-id</td>
<td>(Optional) Neighbor hostname or IP address in A.B.C.D format.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays all neighbors given in detail (lists all neighbors).</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays total number summary of all neighbors.</td>
</tr>
<tr>
<td>per-instance</td>
<td>(Optional) Displays total number of neighbors in each neighbor state. The</td>
</tr>
<tr>
<td></td>
<td>output is printed for each configured OSPF instance separately.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output from the show ip ospf neighbor command shows a single line of summary information for each neighbor:

```
Device# show ip ospf neighbor

Neighbor ID Pri State Dead Time Address Interface
10.199.199.137 1 FULL/DR 0:00:31 192.168.80.37 Ethernet0
172.16.48.1   1 FULL/DROTHER 0:00:33 172.16.48.1  Fddi0
172.16.48.200 1 FULL/DROTHER 0:00:33 172.16.48.200 Fddi0
10.199.199.137 5 FULL/DR 0:00:33 172.16.48.189 Fddi0
```

The following is sample output showing summary information about the neighbor that matches the neighbor ID:

```
Device# show ip ospf neighbor 10.199.199.137

Neighbor 10.199.199.137, interface address 192.168.80.37
  In the area 0.0.0.0 via interface Ethernet0
  Neighbor priority is 1, State is FULL
  Options 2
  Dead timer due in 0:00:32
  Link State retransmission due in 0:00:04
Neighbor 10.199.199.137, interface address 172.16.48.189
  In the area 0.0.0.0 via interface Fddi0
  Neighbor priority is 5, State is FULL
  Options 2
  Dead timer due in 0:00:32
```
Link State retransmission due in 0:00:03

If you specify the interface along with the neighbor ID, the system displays the neighbors that match the neighbor ID on the interface, as in the following sample display:

```
Device# show ip ospf neighbor ethernet 0 10.199.199.137
Neighbor 10.199.199.137, interface address 192.168.80.37
    In the area 0.0.0.0 via interface Ethernet0
    Neighbor priority is 1, State is FULL
    Options 2
    Dead timer due in 0:00:37
    Link State retransmission due in 0:00:04
```

You can also specify the interface without the neighbor ID to show all neighbors on the specified interface, as in the following sample display:

```
Device# show ip ospf neighbor fddi 0

<table>
<thead>
<tr>
<th>ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.48.1</td>
<td>1</td>
<td>FULL/DROTHER</td>
<td>0:00:33</td>
<td>172.16.48.1</td>
<td>Fddi0</td>
</tr>
<tr>
<td>172.16.48.200</td>
<td>1</td>
<td>FULL/DROTHER</td>
<td>0:00:32</td>
<td>172.16.48.200</td>
<td>Fddi0</td>
</tr>
<tr>
<td>10.199.199.137</td>
<td>5</td>
<td>FULL/DR</td>
<td>0:00:32</td>
<td>172.16.48.189</td>
<td>Fddi0</td>
</tr>
</tbody>
</table>
```

The following is sample output from the `show ip ospf neighbor detail` command:

```
Device# show ip ospf neighbor detail
Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface GigabitEthernet1/0/0
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:08 ago
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor</td>
<td>Neighbor router ID.</td>
</tr>
<tr>
<td>interface address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>In the area</td>
<td>Area and interface through which the OSPF neighbor is known.</td>
</tr>
<tr>
<td>Neighbor priority</td>
<td>Router priority of the neighbor and neighbor state.</td>
</tr>
<tr>
<td>State</td>
<td>OSPF state. If one OSPF neighbor has enabled TTL security, the other side of the connection will show the neighbor in the INIT state.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>state changes</td>
<td>Number of state changes since the neighbor was created. This value can be reset using the <code>clearipospfcountersneighbor</code> command.</td>
</tr>
<tr>
<td>DR is</td>
<td>Router ID of the designated router for the interface.</td>
</tr>
<tr>
<td>BDR is</td>
<td>Router ID of the backup designated router for the interface.</td>
</tr>
<tr>
<td>Options</td>
<td>Hello packet options field contents. (E-bit only. Possible values are 0 and 2; 2 indicates area is not a stub; 0 indicates area is a stub.)</td>
</tr>
<tr>
<td>LLS Options... last OOB-Resync</td>
<td>Link-Local Signaling and out-of-band (OOB) link-state database resynchronization performed hours:minutes:seconds ago. This is nonstop forwarding (NSF) information. The field indicates the last successful out-of-band resynchronization with the NSF-capable router.</td>
</tr>
<tr>
<td>Dead timer due in</td>
<td>Expected time in hours:minutes:seconds before Cisco IOS software will declare the neighbor dead.</td>
</tr>
<tr>
<td>Neighbor is up for</td>
<td>Number of hours:minutes:seconds since the neighbor went into the two-way state.</td>
</tr>
<tr>
<td>Index</td>
<td>Neighbor location in the area-wide and autonomous system-wide retransmission queue.</td>
</tr>
<tr>
<td>retransmission queue length</td>
<td>Number of elements in the retransmission queue.</td>
</tr>
<tr>
<td>number of retransmission</td>
<td>Number of times update packets have been re-sent during flooding.</td>
</tr>
<tr>
<td>First</td>
<td>Memory location of the flooding details.</td>
</tr>
<tr>
<td>Next</td>
<td>Memory location of the flooding details.</td>
</tr>
<tr>
<td>Last retransmission scan length</td>
<td>Number of link state advertisements (LSAs) in the last retransmission packet.</td>
</tr>
<tr>
<td>maximum</td>
<td>Maximum number of LSAs sent in any retransmission packet.</td>
</tr>
<tr>
<td>Last retransmission scan time</td>
<td>Time taken to build the last retransmission packet.</td>
</tr>
<tr>
<td>maximum</td>
<td>Maximum time, in milliseconds, taken to build any retransmission packet.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show ip ospf neighbor` command showing a single line of summary information for each neighbor. If one OSPF neighbor has enabled TTL security, the other side of the connection will show the neighbor in the INIT state.

```
Device#show ip ospf neighbor

<table>
<thead>
<tr>
<th>Neighbor ID</th>
<th>Pri</th>
<th>State</th>
<th>Dead Time</th>
<th>Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.199.199.137</td>
<td>1</td>
<td>FULL/DR</td>
<td>0:00:31</td>
<td>192.168.80.37</td>
<td>Ethernet0</td>
</tr>
<tr>
<td>172.16.48.1</td>
<td>1</td>
<td>FULL/DROTHER</td>
<td>0:00:33</td>
<td>172.16.48.1</td>
<td>Fddi0</td>
</tr>
<tr>
<td>172.16.48.200</td>
<td>1</td>
<td>FULL/DROTHER</td>
<td>0:00:33</td>
<td>172.16.48.200</td>
<td>Fddi0</td>
</tr>
</tbody>
</table>
```
Cisco IOS Release 15.1(3)S

The following sample output from the `show ip ospf neighbor` command shows the network from the neighbor’s point of view:

```
Device#show ip ospf neighbor 192.0.2.1
  OSPF Router with ID (192.1.1.1) (Process ID 1)

    Area with ID (0)
    Neighbor with Router ID 192.0.2.1:
    Reachable over:
      Ethernet0/0, IP address 192.0.2.1, cost 10

    SPF was executed 1 times, distance to computing router 10

    Router distance table:
      192.1.1.1   i [10]
      192.0.2.1   i [0]
      192.3.3.3   i [10]
      192.4.4.4   i [20]
      192.5.5.5   i [20]

    Network LSA distance table:
      192.2.12.2   i [10]
      192.2.13.3   i [20]
      192.2.14.4   i [20]
      192.2.15.5   i [20]
```

The following is sample output from the `show ip ospf neighbor summary` command:

```
Device#show ip ospf neighbor summary

    Neighbor summary for all OSPF processes

      DOWN       0
      ATTEMPT    0
      INIT       0
      2WAY       0
      EXSTART    0
      EXCHANGE   0
      LOADING    0
      FULL       1
      Total count 1 (Undergoing NSF 0)
```

The following is sample output from the `show ip ospf neighbor summary per-instance` command:

```
Device#show ip ospf neighbor summary

    OSPF Router with ID (1.0.0.10) (Process ID 1)

      DOWN       0
      ATTEMPT    0
      INIT       0
      2WAY       0
```
### Table 152: `show ip ospf neighbor summary` and `show ip ospf neighbor summary per-instance Field Descriptions`

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOWN</td>
<td>No information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.</td>
</tr>
<tr>
<td>ATTEMPT</td>
<td>This state is only valid for manually configured neighbors in a Non-Broadcast Multi-Access (NBMA) environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.</td>
</tr>
<tr>
<td>INIT</td>
<td>This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.</td>
</tr>
<tr>
<td>2WAY</td>
<td>This state designates that bi-directional communication has been established between two routers.</td>
</tr>
<tr>
<td>EXSTART</td>
<td>This state is the first step in creating an adjacency between the two neighboring routers. The goal of this step is to decide which router is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies.</td>
</tr>
<tr>
<td>EXCHANGE</td>
<td>In this state, OSPF routers exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link-state database to check if new or more current link-state information is available with the neighbor.</td>
</tr>
<tr>
<td>LOADING</td>
<td>In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a device receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>FULL</td>
<td>In this state, devices are fully adjacent with each other. All the device and network LSAs are exchanged and the devices' databases are fully synchronized. Full is the normal state for an OSPF device. If a device is stuck in another state, it's an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Devices achieve the full state with their DR and BDR only. Neighbors always see each other as 2-way.</td>
</tr>
</tbody>
</table>
show ip ospf virtual-links

To display parameters and the current state of Open Shortest Path First (OSPF) virtual links, use the show ip ospf virtual-links command in EXEC mode.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The information displayed by the show ip ospf virtual-links command is useful in debugging OSPF routing operations.

Examples

The following is sample output from the show ip ospf virtual-links command:

```
Device#show ip ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

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

**Table 153: show ip ospf virtual-links Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Link to router 192.168.101.2 is up</td>
<td>Specifies the OSPF neighbor, and if the link to that neighbor is up or down.</td>
</tr>
<tr>
<td>Transit area 0.0.0.1</td>
<td>The transit area through which the virtual link is formed.</td>
</tr>
<tr>
<td>via interface Ethernet0</td>
<td>The interface through which the virtual link is formed.</td>
</tr>
<tr>
<td>Cost of using 10</td>
<td>The cost of reaching the OSPF neighbor through the virtual link.</td>
</tr>
<tr>
<td>Transmit Delay is 1 sec</td>
<td>The transmit delay (in seconds) on the virtual link.</td>
</tr>
<tr>
<td>State POINT_TO_POINT</td>
<td>The state of the OSPF neighbor.</td>
</tr>
<tr>
<td>Timer intervals...</td>
<td>The various timer intervals configured for the link.</td>
</tr>
<tr>
<td>Hello due in 0:00:08</td>
<td>When the next hello is expected from the neighbor.</td>
</tr>
<tr>
<td>Adjacency State FULL</td>
<td>The adjacency state between the neighbors.</td>
</tr>
</tbody>
</table>
summary-address (OSPF)

To create aggregate addresses for Open Shortest Path First (OSPF), use the `summary-address` command in router configuration mode. To restore the default, use the `no` form of this command.

```
summary-address command
summary-address {ip-address mask | prefix mask} [not-advertise] [tag tag] [nssa-only]
no summary-address {ip-address mask | prefix mask} [not-advertise] [tag tag] [nssa-only]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>Summary address designated for a range of addresses.</td>
</tr>
<tr>
<td><code>mask</code></td>
<td>IP subnet mask used for the summary route.</td>
</tr>
<tr>
<td><code>prefix</code></td>
<td>IP route prefix for the destination.</td>
</tr>
<tr>
<td><code>not-advertise</code></td>
<td>(Optional) Suppresses routes that match the specified prefix/mask pair. This keyword applies to OSPF only.</td>
</tr>
<tr>
<td><code>tag tag</code></td>
<td>(Optional) Specifies the tag value that can be used as a “match” value for controlling redistribution via route maps. This keyword applies to OSPF only.</td>
</tr>
<tr>
<td><code>nssa-only</code></td>
<td>(Optional) Sets the nssa-only attribute for the summary route (if any) generated for the specified prefix, which limits the summary to not-so-stubby-area (NSSA) areas.</td>
</tr>
</tbody>
</table>

### Command Default

This command behavior is disabled by default.

### Command Modes

Router configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

Routes learned from other routing protocols can be summarized. The metric used to advertise the summary is the lowest metric of all the more specific routes. This command helps reduce the size of the routing table.

Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. For OSPF, this command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the `area range` command for route summarization between OSPF areas.

OSPF does not support the `summary-address 0.0.0.0 0.0.0.0` command.

### Examples

In the following example, the summary address 10.1.0.0 includes address 10.1.1.0, 10.1.2.0, 10.1.3.0, and so on. Only the address 10.1.0.0 is advertised in an external link-state advertisement.

```
Device(config)#summary-address 10.1.0.0 255.255.0.0
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area range</td>
<td>Consolidates and summarizes routes at an area boundary.</td>
</tr>
<tr>
<td>ip ospf authentication-key</td>
<td>Assigns a password to be used by neighboring routers that are using the simple password authentication of OSPF.</td>
</tr>
<tr>
<td>ip ospf message-digest-key</td>
<td>Enables OSPF MD5 authentication.</td>
</tr>
</tbody>
</table>
**timers throttle spf**

To turn on Open Shortest Path First (OSPF) shortest path first (SPF) throttling, use the `timers throttle spf` command in the appropriate configuration mode. To turn off OSPF SPF throttling, use the `no` form of this command.

```plaintext
timers throttle spf spf-start spf-hold spf-max-wait
no timers throttle spf spf-start spf-hold spf-max-wait
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>spf-start</strong></td>
<td>Initial delay to schedule an SPF calculation after a change, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 5000.</td>
</tr>
<tr>
<td><strong>spf-hold</strong></td>
<td>Minimum hold time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.</td>
</tr>
<tr>
<td><strong>spf-max-wait</strong></td>
<td>Maximum wait time between two consecutive SPF calculations, in milliseconds. Range is from 1 to 600000. In OSPF for IPv6, the default value is 10,000.</td>
</tr>
</tbody>
</table>

**Command Default**

SPF throttling is not set.

**Command Modes**

Address family configuration (config-router-af) 
Router address family topology configuration (config-router-af-topology) 
Router configuration (config-router) 
OSPF for IPv6 router configuration (config-rtr)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The first wait interval between SPF calculations is the amount of time in milliseconds specified by the `spf-start` argument. Each consecutive wait interval is two times the current hold level in milliseconds until the wait time reaches the maximum time in milliseconds as specified by the `spf-max-wait` argument. Subsequent wait times remain at the maximum until the values are reset or a link-state advertisement (LSA) is received between SPF calculations.

**Release 12.2(33)SRB**

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the `timers throttle spf` command in router address family topology configuration mode in order to make this OSPF router configuration command become topology-aware.

**Release 15.2(1)T**

When you configure the `ospfv3 network manet` command on any interface attached to the OSPFv3 process, the default values for the `spf-start`, `spf-hold`, and the `spf-max-wait` arguments are reduced to 1000 milliseconds, 1000 milliseconds, and 2000 milliseconds respectively.

**Examples**

The following example shows how to configure a router with the delay, hold, and maximum interval values for the `timers throttle spf` command set at 5, 1000, and 90,000 milliseconds, respectively.

```plaintext
router ospf 1
router-id 10.10.10.2
```
The following example shows how to configure a router using IPv6 with the delay, hold, and maximum interval values for the `timers throttle spf` command set at 500, 1000, and 10,000 milliseconds, respectively.

```
ipv6 router ospf 1
  event-log size 10000 one-shot
  log-adjacency-changes
  timers throttle spf 500 1000 10000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ospfv3 network manet</td>
<td>Sets the network type to Mobile Ad Hoc Network (MANET).</td>
</tr>
</tbody>
</table>
PART XI

Security

- Security, on page 1215
Security

• aaa accounting, on page 1218
• aaa accounting dot1x, on page 1221
• aaa accounting identity, on page 1223
• aaa authentication dot1x, on page 1225
• aaa authorization, on page 1226
• aaa new-model, on page 1230
• authentication host-mode, on page 1232
• authentication logging verbose, on page 1234
• authentication mac-move permit, on page 1235
• authentication priority, on page 1237
• authentication violation, on page 1240
• cisp enable, on page 1242
• clear errdisable interface vlan, on page 1243
• clear mac address-table, on page 1244
• deny (MAC access-list configuration), on page 1246
• device-role (IPv6 snooping), on page 1250
• device-role (IPv6 nd inspection), on page 1251
• device-tracking policy, on page 1252
• dot1x critical (global configuration), on page 1254
• dot1x logging verbose, on page 1255
• dot1x max-start, on page 1256
• dot1x pae, on page 1257
• dot1x supplicant controlled transient, on page 1258
• dot1x supplicant force-multicast, on page 1259
• dot1x test eapol-capable, on page 1260
• dot1x test timeout, on page 1261
• dot1x timeout, on page 1262
• dtls, on page 1264
• enable password, on page 1266
• enable secret, on page 1269
• epm access-control open, on page 1272
• ip access-list role-based, on page 1273
• ip admission, on page 1274
• ip admission name, on page 1275
• ip dhcp snooping database, on page 1277
• ip dhcp snooping information option format remote-id, on page 1279
• ip dhcp snooping verify no-relay-agent-address, on page 1280
• ip http access-class, on page 1281
• ip radius source-interface, on page 1283
• ip source binding, on page 1285
• ip ssh source-interface, on page 1286
• ip verify source, on page 1287
• ipv6 access-list, on page 1288
• ipv6 snooping policy, on page 1290
• key chain macsec, on page 1291
• key config-key password-encrypt, on page 1292
• limit address-count, on page 1294
• mab logging verbose, on page 1295
• mab request format attribute 32, on page 1296
• macsec network-link, on page 1298
• match (access-map configuration), on page 1299
• mka pre-shared-key, on page 1301
• mka suppress syslogs sak-rekey, on page 1302
• password encryption aes, on page 1303
• permit (MAC access-list configuration), on page 1305
• protocol (IPv6 snooping), on page 1309
• radius server, on page 1310
• security level (IPv6 snooping), on page 1312
• security passthru, on page 1313
• server-private (RADIUS), on page 1314
• show aaa clients, on page 1316
• show aaa command handler, on page 1317
• show aaa local, on page 1318
• show aaa servers, on page 1320
• show aaa sessions, on page 1321
• show authentication brief, on page 1322
• show authentication history, on page 1325
• show authentication sessions, on page 1326
• show cisp, on page 1329
• show dot1x, on page 1331
• show eap pac peer, on page 1333
• show ip dhcp snooping statistics, on page 1334
• show radius server-group, on page 1337
• show storm-control, on page 1339
• show tech-support acl, on page 1341
• show tech-support identity, on page 1345
• show vlan access-map, on page 1354
• show vlan filter, on page 1355
• show vlan group, on page 1356
• storm-control, on page 1357
• switchport port-security aging, on page 1360
• switchport port-security mac-address, on page 1362
• switchport port-security maximum, on page 1365
• switchport port-security violation, on page 1367
• tacacs server, on page 1369
• tracking (IPv6 snooping), on page 1370
• trusted-port, on page 1372
• username, on page 1373
• vlan access-map, on page 1378
• vlan filter, on page 1380
• vlan group, on page 1381
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.

```markdown
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.
- **list-name**: 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.
- **group group-name**: At least one of the keywords described in the AAA Accounting Methods table.

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration (config)
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 154: AAA Accounting Methods**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication as defined by the <code>aaa group server radius</code> command.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication as defined by the <code>aaa group server tacacs+</code> command.</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name.</td>
</tr>
</tbody>
</table>

In AAA Accounting Methods table, 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 XE 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.

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.

---

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> enable
Device# configure terminal
Device(config)# aaa accounting commands 15 default stop-only group TACACS+
Device(config)# exit
```

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> enable
Device# configure terminal
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+
Device(config)# exit
```
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 device 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 (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**Security**

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa accounting dot1x default start-stop group radius
Device(config)# exit
```
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+} ... ]}
no aaa accounting identity {name | default}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of a server group. This is optional when you enter it after the <code>broadcast group</code> and <code>group</code> keywords.</td>
</tr>
<tr>
<td>default</td>
<td>Uses the accounting methods that follow as the default list for accounting services.</td>
</tr>
<tr>
<td>start-stop</td>
<td>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.</td>
</tr>
<tr>
<td>broadcast</td>
<td>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.</td>
</tr>
<tr>
<td>group</td>
<td>Specifies the server group to be used for accounting services. These are valid server group names:</td>
</tr>
<tr>
<td></td>
<td>• <code>name</code> — Name of a server group.</td>
</tr>
<tr>
<td></td>
<td>• <code>radius</code> — Lists all RADIUS hosts.</td>
</tr>
<tr>
<td></td>
<td>• <code>tacacs+</code> — Lists all TACACS+ hosts.</td>
</tr>
<tr>
<td>radius</td>
<td>(Optional) Enables RADIUS authorization.</td>
</tr>
<tr>
<td>tacacs+</td>
<td>(Optional) Enables TACACS+ accounting.</td>
</tr>
</tbody>
</table>

### Command Default

AAA accounting is disabled.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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
Device(config)# exit
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. To disable authentication, use the `no` form of this command.

```
aaa authentication dot1x {default} method1
no aaa authentication dot1x {default} method1
```

**Syntax Description**

- **default**: The default method when a user logs in. Use the listed authentication method that follows this argument.
- **method1**: Specifies the server authentication. Enter the `group radius` keywords to use the list of all RADIUS servers for authentication.

**Note**: Though other keywords are visible in the command-line help strings, only the `default` and `group radius` keywords are supported.

**Command Default**

No authentication is performed.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Everest 16.5.1a | 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> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius
Device(config)# exit
```
## 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.

```plaintext
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-proxy</td>
<td>Runs authorization for authentication proxy services.</td>
</tr>
<tr>
<td>cache</td>
<td>Configures the authentication, authorization, and accounting (AAA) server.</td>
</tr>
<tr>
<td>commands</td>
<td>Runs authorization for all commands at the specified privilege level.</td>
</tr>
<tr>
<td>level</td>
<td>Specific command level that should be authorized. Valid entries are 0 through 15.</td>
</tr>
<tr>
<td>config-commands</td>
<td>Runs authorization to determine whether commands entered in configuration mode are authorized.</td>
</tr>
<tr>
<td>configuration</td>
<td>Downloads the configuration from the AAA server.</td>
</tr>
<tr>
<td>console</td>
<td>Enables the console authorization for the AAA server.</td>
</tr>
<tr>
<td>credential-download</td>
<td>Downloads EAP credential from Local/RADIUS/LDAP.</td>
</tr>
<tr>
<td>exec</td>
<td>Enables the console authorization for the AAA server.</td>
</tr>
<tr>
<td>multicast</td>
<td>Downloads the multicast configuration from the AAA server.</td>
</tr>
<tr>
<td>network</td>
<td>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).</td>
</tr>
<tr>
<td>reverse-access</td>
<td>Runs authorization for reverse access connections, such as reverse Telnet.</td>
</tr>
<tr>
<td>template</td>
<td>Enables template authorization for the AAA server.</td>
</tr>
<tr>
<td>default</td>
<td>Uses the listed authorization methods that follow this keyword as the default list of methods for authorization.</td>
</tr>
<tr>
<td>list_name</td>
<td>Character string used to name the list of authorization methods.</td>
</tr>
<tr>
<td>method1 [ method2... ]</td>
<td>(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.</td>
</tr>
</tbody>
</table>
Command Default

Authorization is disabled for all actions (equivalent to the method keyword none).

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 XE software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS XE 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 XE 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>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cache group-name</code></td>
<td>Uses a cache server group for authorization.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>group group-name</td>
<td>Uses a subset of RADIUS or TACACS+ servers for accounting as defined by the server group group-name command.</td>
</tr>
<tr>
<td>group ldap</td>
<td>Uses the list of all Lightweight Directory Access Protocol (LDAP) servers for authentication.</td>
</tr>
<tr>
<td>group radius</td>
<td>Uses the list of all RADIUS servers for authentication as defined by the aaa group server radius command.</td>
</tr>
<tr>
<td>group tacacs+</td>
<td>Uses the list of all TACACS+ servers for authentication as defined by the aaa group server tacacs+ command.</td>
</tr>
</tbody>
</table>
| 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 XE software supports the following methods for authorization:

- **Cache Server Groups**—The device 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 device 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.

• 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> enable
Device# configure terminal
Device(config)# aaa authorization network mygroup group radius local
Device(config)# exit
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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

### Examples

The following example initializes AAA:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# exit
```

The following example shows a VTY configured and the `aaa new-model` command removed:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# line vty 0 15
Device(config-line)# login local
Device(config-line)# exit
Device(config)# no aaa new-model
Device(config)# exit
Device# show running-config | b line vty

line vty 0 4
login local !<--- Login local instead of "login"
line vty 5 15
login local
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa accounting</td>
<td>Enables AAA accounting of requested services for billing or security purposes.</td>
</tr>
<tr>
<td>aaa authentication arap</td>
<td>Enables an AAA authentication method for ARAP using TACACS+.</td>
</tr>
<tr>
<td>aaa authentication enable default</td>
<td>Enables AAA authentication to determine if a user can access the privileged command level.</td>
</tr>
<tr>
<td>aaa authentication login</td>
<td>Sets AAA authentication at login.</td>
</tr>
<tr>
<td>aaa authentication ppp</td>
<td>Specifies one or more AAA authentication method for use on serial interfaces running PPP.</td>
</tr>
<tr>
<td>aaa authorization</td>
<td>Sets parameters that restrict user access to a network.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>multi-auth</code></td>
<td>Enables multiple-authorization mode (multi-auth mode) on the port.</td>
</tr>
<tr>
<td><code>multi-domain</code></td>
<td>Enables multiple-domain mode on the port.</td>
</tr>
<tr>
<td><code>multi-host</code></td>
<td>Enables multiple-host mode on the port.</td>
</tr>
<tr>
<td><code>single-host</code></td>
<td>Enables single-host mode on the port.</td>
</tr>
</tbody>
</table>

**Command Default**

Single host mode is enabled.

**Command Modes**

`Interface configuration (config-if)`

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication host-mode multi-auth
Device(config-if)# end
```

This example shows how to enable multi-domain mode on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
```

Device(config-if)# **authentication host-mode multi-domain**
Device(config-if)# **end**

This example shows how to enable multi-host mode on a port:

Device> **enable**
Device# **configure terminal**
Device(config)# **interface gigabitethernet 2/0/1**
Device(config-if)# **authentication host-mode multi-host**
Device(config-if)# **end**

This example shows how to enable single-host mode on a port:

Device> **enable**
Device# **configure terminal**
Device(config)# **interface gigabitethernet 2/0/1**
Device(config-if)# **authentication host-mode single-host**
Device(config-if)# **end**

You can verify your settings by entering the **show authentication sessions interface interface details** privileged EXEC command.
authentication logging verbose

To filter detailed information from authentication system messages, use the authentication logging verbose command in global configuration mode on the switch stack or on a standalone switch.

```
authentication logging verbose
no authentication logging verbose
```

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

**Command Default**
Detailed logging of system messages is not enabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# authentication logging verbose
Device(config)# exit
```

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

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication logging verbose</td>
<td>Filters details from authentication system messages.</td>
</tr>
<tr>
<td>dot1x logging verbose</td>
<td>Filters details from 802.1x system messages.</td>
</tr>
<tr>
<td>mab logging verbose</td>
<td>Filters details from MAC authentication bypass (MAB) system messages.</td>
</tr>
</tbody>
</table>
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.

```plaintext
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 (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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:

```plaintext
Device> enable
Device# configure terminal
Device(config)# authentication mac-move permit
Device(config)# exit
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-session mac-move deny</td>
<td>Disables MAC move on a device.</td>
</tr>
<tr>
<td>authentication event</td>
<td>Sets the action for specific authentication events.</td>
</tr>
<tr>
<td>authentication fallback</td>
<td>Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>Sets the authorization manager mode on a port.</td>
</tr>
<tr>
<td>authentication open</td>
<td>Enables or disables open access on a port.</td>
</tr>
<tr>
<td>authentication order</td>
<td>Sets the order of authentication methods used on a port.</td>
</tr>
<tr>
<td>authentication periodic</td>
<td>Enable or disables reauthentication on a port.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>authentication port-control</td>
<td>Enables manual control of the port authorization state.</td>
</tr>
<tr>
<td>authentication priority</td>
<td>Adds an authentication method to the port-priority list.</td>
</tr>
<tr>
<td>authentication timer</td>
<td>Configures the timeout and reauthentication parameters for an 802.1x-enabled port.</td>
</tr>
<tr>
<td>authentication violation</td>
<td>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.</td>
</tr>
<tr>
<td>show authentication</td>
<td>Displays information about authentication manager events on the device.</td>
</tr>
</tbody>
</table>
**authentication priority**

To add an authentication method to the port-priority list, use the `authentication priority` command in interface configuration mode. To return to the default, use the `no` form of this command.

```
authentication priority [dot1x | mab] {webauth}
no authentication priority [dot1x | mab] {webauth}
```

**Syntax Description**

- `dot1x` (Optional) Adds 802.1x to the order of authentication methods.
- `mab` (Optional) Adds MAC authentication bypass (MAB) to the order of authentication methods.
- `webauth` Adds web authentication to the order of authentication methods.

**Command Default**

The default priority is 802.1x authentication, followed by MAC authentication bypass and web authentication.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Ordering sets the order of methods that the device attempts when trying to authenticate a new device is connected to a port.

When configuring multiple fallback methods on a port, set web authentication (webauth) last.

Assigning priorities to different authentication methods allows a higher-priority method to interrupt an in-progress authentication method with a lower priority.

*Note*

If a client is already authenticated, it might be reauthenticated if an interruption from a higher-priority method occurs.

The default priority of an authentication method is equivalent to its position in execution-list order: 802.1x authentication, MAC authentication bypass (MAB), and web authentication. Use the `dot1x`, `mab`, and `webauth` keywords to change this default order.

This example shows how to set 802.1x as the first authentication method and web authentication as the second authentication method:

```
Device(config-if)# authentication priority dot1x webauth
```

This example shows how to set MAB as the first authentication method and web authentication as the second authentication method:
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 0/1/2
Device(config-if)# authentication priority mab webauth
Device(config-if)# end

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication control-direction</td>
<td>Configures the port mode as unidirectional or bidirectional.</td>
</tr>
<tr>
<td>authentication event fail</td>
<td>Specifies how the Auth Manager handles authentication failures as a result of unrecognized user credentials.</td>
</tr>
<tr>
<td>authentication event no-response action</td>
<td>Specifies how the Auth Manager handles authentication failures as a result of a nonresponsive host.</td>
</tr>
<tr>
<td>authentication event server alive action reinitialize</td>
<td>Reinitializes an authorized Auth Manager session when a previously unreachable authentication, authorization, and accounting server becomes available.</td>
</tr>
<tr>
<td>authentication event server dead action authorize</td>
<td>Authorizes Auth Manager sessions when the authentication, authorization, and accounting server becomes unreachable.</td>
</tr>
<tr>
<td>authentication fallback</td>
<td>Enables a web authentication fallback method.</td>
</tr>
<tr>
<td>authentication host-mode</td>
<td>Allows hosts to gain access to a controlled port.</td>
</tr>
<tr>
<td>authentication open</td>
<td>Enables open access on a port.</td>
</tr>
<tr>
<td>authentication order</td>
<td>Specifies the order in which the Auth Manager attempts to authenticate a client on a port.</td>
</tr>
<tr>
<td>authentication periodic</td>
<td>Enables automatic reauthentication on a port.</td>
</tr>
<tr>
<td>authentication port-control</td>
<td>Configures the authorization state of a controlled port.</td>
</tr>
<tr>
<td>authentication timer inactivity</td>
<td>Configures the time after which an inactive Auth Manager session is terminated.</td>
</tr>
<tr>
<td>authentication timer reauthenticate</td>
<td>Specifies the period of time between which the Auth Manager attempts to reauthenticate authorized ports.</td>
</tr>
<tr>
<td>authentication timer restart</td>
<td>Specifies the period of time after which the Auth Manager attempts to authenticate an unauthorized port.</td>
</tr>
<tr>
<td>authentication violation</td>
<td>Specifies the action to be taken when a security violation occurs on a port.</td>
</tr>
<tr>
<td>mab</td>
<td>Enables MAC authentication bypass on a port.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>show authentication registrations</code></td>
<td>Displays information about the authentication methods that are registered with the Auth Manager.</td>
</tr>
<tr>
<td><code>show authentication sessions</code></td>
<td>Displays information about current Auth Manager sessions.</td>
</tr>
<tr>
<td><code>show authentication sessions interface</code></td>
<td>Displays information about the Auth Manager for a given interface.</td>
</tr>
</tbody>
</table>
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  }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>protect</th>
<th>Drops unexpected incoming MAC addresses. No syslog errors are generated.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>replace</td>
<td>Removes the current session and initiates authentication with the new host.</td>
</tr>
<tr>
<td></td>
<td>restrict</td>
<td>Generates a syslog error when a violation error occurs.</td>
</tr>
<tr>
<td></td>
<td>shutdown</td>
<td>Error-disables the port or the virtual port on which an unexpected MAC address occurs.</td>
</tr>
</tbody>
</table>

**Command Default**

Authentication violation shutdown mode is enabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation shutdown
Device(config-if)# end
```

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation restrict
Device(config-if)# end
```

This example shows how to configure an 802.1x-enabled port to ignore a new device when it connects to the port:
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation protect
Device(config-if)# end

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 2/0/1
Device(config-if)# authentication violation replace
Device(config-if)# end

You can verify your settings by entering the show authentication command.
**cisp enable**

To enable Client Information Signaling Protocol (CISP) on a device so that it acts as an authenticator to a supplicant device and a supplicant to an authenticator device, 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 (config)

**Command History**
The link between the authenticator and supplicant device is a trunk. When you enable VTP on both devices, 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 devices, which can be caused by two VTP servers in the same domain.
- Both devices have different configuration revision numbers.

This example shows how to enable CISP:

```
Device> enable
Device# configure terminal
Device(config)# cisp enable
Device(config)# exit
```

**Usage Guidelines**

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x credentials profile</code></td>
<td>Configures a profile on a supplicant device.</td>
</tr>
<tr>
<td><code>dot1x supplicant force-multicast</code></td>
<td>Forces 802.1X supplicant to send multicast packets.</td>
</tr>
<tr>
<td><code>dot1x supplicant controlled transient</code></td>
<td>Configures controlled access by 802.1X supplicant.</td>
</tr>
<tr>
<td><code>show cisp</code></td>
<td>Displays CISP information for a specified interface.</td>
</tr>
</tbody>
</table>
clear errdisable interface vlan

To reenable a VLAN that was error-disabled, use the **clear errdisable interface** command in privileged EXEC mode.

```
clear errdisable interface interface-id vlan [vlan-list]
```

**Syntax Description**

- `interface-id`: Specifies an interface.
- `vlan list`: (Optional) Specifies a list of VLANs to be reenabled. If a VLAN list is not specified, then all VLANs are reenabled.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can reenable a port by using the `shutdown` and `no shutdown` interface configuration commands, or you can clear error-disable for VLANs by using the **clear errdisable interface** command.

This example shows how to reenable all VLANs that were error-disabled on Gigabit Ethernet port 4/0/2:

```
Device# clear errdisable interface gigabitethernet4/0/2 vlan
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>errdisable detect cause</code></td>
<td>Enables error-disabled detection for a specific cause or all causes.</td>
</tr>
<tr>
<td><code>errdisable recovery</code></td>
<td>Configures the recovery mechanism variables.</td>
</tr>
<tr>
<td><code>show errdisable detect</code></td>
<td>Displays error-disabled detection status.</td>
</tr>
<tr>
<td><code>show errdisable recovery</code></td>
<td>Displays error-disabled recovery timer information.</td>
</tr>
<tr>
<td><code>show interfaces status err-disabled</code></td>
<td>Displays interface status of a list of interfaces in error-disabled state.</td>
</tr>
</tbody>
</table>

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dynamic</td>
<td>Deletes all dynamic MAC addresses.</td>
</tr>
<tr>
<td>address mac-addr</td>
<td>(Optional) Deletes the specified dynamic MAC address.</td>
</tr>
<tr>
<td>interface interface-id</td>
<td>(Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel.</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>(Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094.</td>
</tr>
<tr>
<td>move update</td>
<td>Clears the MAC address table move-update counters.</td>
</tr>
<tr>
<td>notification</td>
<td>Clears the notifications in the history table and reset the counters.</td>
</tr>
</tbody>
</table>

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You can verify that the information was deleted by entering the show mac address-table command.

This example shows how to remove a specific MAC address from the dynamic address table:

```
Device> enable
Device# clear mac address-table dynamic address 0008.0070.0007
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mac address-table</code></td>
<td>Displays the MAC address table static and dynamic entries.</td>
</tr>
<tr>
<td><code>show mac address-table move update</code></td>
<td>Displays the MAC address-table move update information on the device.</td>
</tr>
<tr>
<td><code>show mac address-table notification</code></td>
<td>Displays the MAC address notification settings for all interfaces or on the specified interface when the <code>interface</code> keyword is appended.</td>
</tr>
<tr>
<td><code>snmp trap mac-notification change</code></td>
<td>Enables the SNMP MAC address notification trap on a specific interface.</td>
</tr>
</tbody>
</table>
deny (MAC access-list configuration)

To prevent non-IP traffic from being forwarded if the conditions are matched, use the `deny` command in MAC access-list extended configuration mode. 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 | lave-sca | lsap | lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp] [cos cos]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>deny</code></td>
<td>Denies any source or destination MAC address.</td>
</tr>
<tr>
<td><code>any</code></td>
<td>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.</td>
</tr>
<tr>
<td>`host src-MAC-addr</td>
<td>src-MAC-addr mask`</td>
</tr>
<tr>
<td><code>type mask</code></td>
<td>(Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.</td>
</tr>
<tr>
<td><code>aarp</code></td>
<td>(Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address.</td>
</tr>
<tr>
<td><code>amber</code></td>
<td>(Optional) Specifies EtherType DEC-Amber.</td>
</tr>
<tr>
<td><code>appletalk</code></td>
<td>(Optional) Specifies EtherType AppleTalk/EtherTalk.</td>
</tr>
<tr>
<td><code>dec-spanning</code></td>
<td>(Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree.</td>
</tr>
<tr>
<td><code>decnet-iv</code></td>
<td>(Optional) Specifies EtherType DECnet Phase IV protocol.</td>
</tr>
<tr>
<td><code>diagnostic</code></td>
<td>(Optional) Specifies EtherType DEC-Diagnostic.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>dsm</td>
<td>(Optional) Specifies EtherType DEC-DSM.</td>
</tr>
<tr>
<td>etype-6000</td>
<td>(Optional) Specifies EtherType 0x6000.</td>
</tr>
<tr>
<td>etype-8042</td>
<td>(Optional) Specifies EtherType 0x8042.</td>
</tr>
<tr>
<td>lat</td>
<td>(Optional) Specifies EtherType DEC-LAT.</td>
</tr>
<tr>
<td>lavc-sca</td>
<td>(Optional) Specifies EtherType DEC-LAVC-SCA.</td>
</tr>
<tr>
<td>lsap lsap-number mask</td>
<td>(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet. A mask is a mask of don’t care bits applied to the LSAP number before testing for a match.</td>
</tr>
<tr>
<td>mop-console</td>
<td>(Optional) Specifies EtherType DEC-MOP Remote Console.</td>
</tr>
<tr>
<td>mop-dump</td>
<td>(Optional) Specifies EtherType DEC-MOP Dump.</td>
</tr>
<tr>
<td>msdos</td>
<td>(Optional) Specifies EtherType DEC-MSDOS.</td>
</tr>
<tr>
<td>mumps</td>
<td>(Optional) Specifies EtherType DEC-MUMPS.</td>
</tr>
<tr>
<td>netbios</td>
<td>(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).</td>
</tr>
<tr>
<td>vines-echo</td>
<td>(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.</td>
</tr>
<tr>
<td>vines-ip</td>
<td>(Optional) Specifies EtherType VINES IP.</td>
</tr>
<tr>
<td>xns-idp</td>
<td>(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary EtherType in decimal, hexadecimal, or octal.</td>
</tr>
<tr>
<td>cos cos</td>
<td>(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.</td>
</tr>
</tbody>
</table>

**Command Default**
This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**
MAC-access list extended configuration (config-ext-macl)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
You enter MAC-access list extended 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 XE terminology are listed in the table.

**Table 156: IPX Filtering Criteria**

<table>
<thead>
<tr>
<th>IPX Encapsulation Type</th>
<th>Filter Criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Name</td>
<td>Novel Name</td>
</tr>
<tr>
<td>arpa</td>
<td>Ethernet II</td>
</tr>
<tr>
<td>snap</td>
<td>Ethernet-snap</td>
</tr>
<tr>
<td>sap</td>
<td>Ethernet 802.2</td>
</tr>
<tr>
<td>novell-ether</td>
<td>Ethernet 802.3</td>
</tr>
</tbody>
</table>

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> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
Device(config-ext-macl)# end
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
Device(config-ext-macl)# end
```

The following example shows how to deny all packets with EtherType 0x4321:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended mac_layer
Device(config-ext-macl)# deny any any 0x4321 0
Device(config-ext-macl)# end
```

You can verify your settings by entering the `show access-lists` privileged EXEC command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac access-list extended</td>
<td>Creates an access list based on MAC addresses for non-IP traffic.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits from the MAC access-list configuration. Permits non-IP traffic to be forwarded if conditions are matched.</td>
</tr>
<tr>
<td>show access-lists</td>
<td>Displays access control lists configured on a device.</td>
</tr>
</tbody>
</table>
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. To remove the specification, use the `no` form of this command.

```
device-role { node | switch }
no 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 device.

**Command Default**
The device role is node.

**Command Modes**
IPv6 snooping configuration (config-ipv6-snooping)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The `device-role` command specifies the role of the device attached to the port. By default, the device role is node.

The `switch` keyword indicates that the remote device is a switch and that the local switch is now operating in multiswitch mode; binding entries learned from the port will be marked with trunk_port preference level. If the port is configured as a trust-port, binding entries will be marked with trunk_trusted_port preference level.

This example shows how to define an IPv6 snooping policy name as `policy1`, place the device in IPv6 snooping configuration mode, and configure the device as the node:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# device-role node
Device(config-ipv6-snooping)# end
```
**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 (config-nd-inspection)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# device-role host
Device(config-nd-inspection)# end
```
device-tracking policy

To configure a Switch Integrated Security Features (SISF)-based IP device tracking policy, use the device-tracking command in global configuration mode. To delete a device tracking policy, use the no form of this command.

```
device-tracking policy policy-name
no device-tracking policy policy-name
```

### Syntax Description

- **policy-name**: User-defined name of the device tracking policy. The policy name can be a symbolic string (such as Engineering) or an integer (such as 0).

### Command Default

A device tracking policy is not configured.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 device-tracking policy:

```
Device> enable
Device# configure terminal
Device(config)# device-tracking policy policy1
Device(config-device-tracking)# trusted-port
Device(config-device-tracking)# end
```
**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 device successfully authenticates the critical port.

**Command Default**

eapol is disabled

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to specify that the device sends an EAPOL-Success message when the device successfully authenticates the critical port:

```
Device> enable
Device# configure terminal
Device(config)# dot1x critical eapol
Device(config)# exit
```
dot1x logging verbose

To filter detailed information from 802.1x system messages, use the **dot1x logging verbose** command in global configuration mode on a device stack or on a standalone device.

**dot1x logging verbose**

**no dot1x logging verbose**

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

**Command Default**
Detailed logging of system messages is not enabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command filters details, such as anticipated success, from 802.1x system messages. Failure messages are not filtered.

The following example shows how to filter verbose 802.1x system messages:

```
Device> enable
Device# configure terminal
Device(config)# dot1x logging verbose
Device(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>authentication logging verbose</strong></td>
<td>Filters details from authentication system messages.</td>
</tr>
<tr>
<td><strong>dot1x logging verbose</strong></td>
<td>Filters details from 802.1x system messages.</td>
</tr>
<tr>
<td><strong>mab logging verbose</strong></td>
<td>Filters details from MAC authentication bypass (MAB) system messages.</td>
</tr>
</tbody>
</table>
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 (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You must enter the `switchport mode access` 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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x max-start 5
Device(config-if)# end
```
**dot1x pae**

To set the Port Access Entity (PAE) type, use the `dot1x pae` command in interface configuration mode. To disable the PAE type that was set, use the `no` form of this command.

```
dot1x pae {supplicant | authenticator}
no dot1x pae {supplicant | authenticator}
```

| Syntax Description | supplicant | 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.

**Command Default**

PAE type is not set.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Cisco IOS XE Everest 16.5.1a | This command was introduced.

**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 device 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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/3
Device(config-if)# dot1x pae supplicant
Device(config-if)# end
```
**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.

**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 (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In the default state, when you connect a supplicant device 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. You can control traffic exiting the supplicant port during the authentication period. Entering the **dot1x supplicant controlled transient** 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** command opens the supplicant port during the authentication period. This is the default behavior.

We recommend using the **dot1x supplicant controlled transient** command on a supplicant device 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 device during authentication:

```
Device> enable
Device# configure terminal
Device(config)# dot1x supplicant controlled transient
Device(config)# exit
```
**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 device 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 (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enable this command on the supplicant device for Network Edge Access Topology (NEAT) to work in all host modes.

This example shows how force a supplicant device to send multicast EAPOL packets to the authenticator device:

```
Device> enable
Device# configureterminal
Device(config)# dot1x supplicant force-multicast
Device(config)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisp enable</td>
<td>Enables CISP on a device so that it acts as an authenticator to a supplicant switch.</td>
</tr>
<tr>
<td>dot1x credentials</td>
<td>Configures the 802.1x supplicant credentials on the port.</td>
</tr>
<tr>
<td>dot1x pae supplicant</td>
<td>Configures an interface to act only as a supplicant.</td>
</tr>
</tbody>
</table>
**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.

```
    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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x test timeout timeout</code></td>
<td>Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query.</td>
</tr>
</tbody>
</table>
**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.

```
dot1x test timeout timeout
```

**Syntax Description**

| `timeout` | Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds. |

**Command Default**
The default setting is 10 seconds.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the `show running-config` command.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dot1x test eapol-capable [interface interface-id]</code></td>
<td>Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports.</td>
</tr>
</tbody>
</table>
# 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-period</td>
<td>Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 30.</td>
</tr>
<tr>
<td>held-period</td>
<td>Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). The range is from 1 to 65535. The default is 60.</td>
</tr>
<tr>
<td>quiet-period</td>
<td>Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. The range is from 1 to 65535. The default is 60.</td>
</tr>
</tbody>
</table>
| ratelimit-period | 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 device processing power).  
  • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration.  
  • The range is from 1 to 65535. By default, rate limiting is disabled. |
| server-timeout | Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted.  
  • The range is from 1 to 65535. The default is 30. |
| start-period   | Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. The range is from 1 to 65535. The default is 30. |

If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
Supp-timeout seconds

Sets the authenticator-to-suppliant 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

Global configuration (config)
Interface configuration (config-if)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 device only if you have enabled periodic re-authentication by using the `dot1x reauthentication` interface configuration command.

During the quiet period, the device 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 device 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> enable
Device(config)# configure terminal
Device(config)# interface gigabitethernet 1/0/3
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
Device(config-if)# end
```
To configure Datagram Transport Layer Security (DTLS) parameters, use the `dtls` command in radius server configuration mode. To return to the default setting, use the `no` form of this command.

```
dtls [connectiontimeout connection-timeout-value] [idletimeout idle-timeout-value] [ip {radius source-interface interface-name | vrf forwarding forwarding-table-name}] [port port-number] [retries number-of-connection-retries] [trustpoint {client trustpoint name | server trustpoint name}]
```

**no dtls**

### Syntax Description

- **connectiontimeout connection-timeout-value** (Optional) Configures the DTLS connection timeout value.
- **idletimeout idle-timeout-value** (Optional) Configures the DTLS idle timeout value.
- **ip {radius source-interface interface-name | vrf forwarding forwarding-table-name}** (Optional) Configures IP source parameters.
- **port port-number** (Optional) Configures the DTLS port number.
- **retries number-of-connection-retries** (Optional) Configures the number of DTLS connection retries.
- **trustpoint {client trustpoint name | server trustpoint name}** (Optional) Configures the DTLS trustpoint for the client and the server.

### Command Default

- The default value of DTLS connection timeout is 5 seconds.
- The default value of DTLS idle timeout is 60 seconds.
- The default DTLS port number is 2083.
- The default value of DTLS connection retries is 5.

### Command Modes

- Radius server configuration (config-radius-server)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

We recommend that you use the same server type, either only Transport Layer Security (TLS) or only DTLS, under an Authentication, Authorization, and Accounting (AAA) server group.

### Examples

The following example shows how to configure the DTLS connection timeout value to 10 seconds:

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
```

---

**dtls**

To configure Datagram Transport Layer Security (DTLS) parameters, use the `dtls` command in radius server configuration mode. To return to the default setting, use the `no` form of this command.

```
dtls [connectiontimeout connection-timeout-value] [idletimeout idle-timeout-value] [ip {radius source-interface interface-name | vrf forwarding forwarding-table-name}] [port port-number] [retries number-of-connection-retries] [trustpoint {client trustpoint name | server trustpoint name}]
```

**no dtls**

### Syntax Description

- **connectiontimeout connection-timeout-value** (Optional) Configures the DTLS connection timeout value.
- **idletimeout idle-timeout-value** (Optional) Configures the DTLS idle timeout value.
- **ip {radius source-interface interface-name | vrf forwarding forwarding-table-name}** (Optional) Configures IP source parameters.
- **port port-number** (Optional) Configures the DTLS port number.
- **retries number-of-connection-retries** (Optional) Configures the number of DTLS connection retries.
- **trustpoint {client trustpoint name | server trustpoint name}** (Optional) Configures the DTLS trustpoint for the client and the server.

### Command Default

- The default value of DTLS connection timeout is 5 seconds.
- The default value of DTLS idle timeout is 60 seconds.
- The default DTLS port number is 2083.
- The default value of DTLS connection retries is 5.

### Command Modes

- Radius server configuration (config-radius-server)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

We recommend that you use the same server type, either only Transport Layer Security (TLS) or only DTLS, under an Authentication, Authorization, and Accounting (AAA) server group.

### Examples

The following example shows how to configure the DTLS connection timeout value to 10 seconds:

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
```
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# end

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show aaa servers</td>
<td>Displays information related to the DTLS server.</td>
</tr>
<tr>
<td>clear aaa counters servers radius {server id</td>
<td>all}</td>
</tr>
<tr>
<td>debug radius dtls</td>
<td>Enables RADIUS DTLS-specific debugs.</td>
</tr>
</tbody>
</table>
enable password

To set a local password to control access to various privilege levels, use the enable password command in global configuration mode. To remove control access of the local password, use the no form of this command.

enable password [level level] { [0] unencrypted-password | [ encryption-type] encrypted-password} no enable password [level level]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level level</td>
<td>(Optional) Specifies the level for which the password is applicable. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal user EXEC mode user privileges. If level is not specified in the command or in the no form of the command, the privilege level defaults to 15.</td>
</tr>
<tr>
<td>0</td>
<td>(Optional) Specifies an unencrypted cleartext password. The password is converted to a Secure Hash Algorithm (SHA) 256 secret and is stored in the device.</td>
</tr>
<tr>
<td>unencrypted-password</td>
<td>Specifies the password to enter enable mode.</td>
</tr>
<tr>
<td>encryption-type</td>
<td>(Optional) Cisco-proprietary algorithm used to encrypt the password. If you specify encryption-type, the next argument that you supply must be an encrypted password (a password already encrypted by a Cisco device). You can specify type 7, which indicates that a hidden password follows.</td>
</tr>
<tr>
<td>encrypted-password</td>
<td>Encrypted password copied from another device configuration.</td>
</tr>
</tbody>
</table>

Command Default

No password is defined.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If neither the enable password command nor the enable secret command is configured, and if a line password is configured for the console, the console line password serves as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use enable password command with the level option to define a password for a specific privilege level. After you specify the level and the password, share the password with users who need to access this level. Use the privilege level configuration command to specify the commands that are accessible at various levels.

Typically, you enter an encryption type only if you copy and paste a password that has already been encrypted by a Cisco device, into this command.
If you specify an encryption type and then enter a cleartext password, you will not be able to re-enter enable mode. You cannot recover a lost password that has been encrypted earlier.

Caution

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when the **more nvram:startup-config** command is run.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain a combination of numerals from 1 to 25, and uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-V when you create the password, for example, to create the password `abc?123`, do the following:
  1. Enter `abc`.
  2. Press Ctrl-v.
  3. Enter `?123`.

Note

When the system prompt you to enter the **enable password** command, you need not precede the question mark with Ctrl-V; you can enter `abc?123` at the password prompt.

Examples

The following example shows how to enable the password `pswd2` for privilege level 2:

```plaintext
Device> enable
Device# configure terminal
Device(config)# enable password level 2 pswd2
```

The following example shows how to set the encrypted password `$1$i5Rkls3LoyxzS8t9`, which has been copied from a device configuration file, for privilege level 2 using encryption type 7:

```plaintext
Device> enable
Device# configure terminal
Device(config)# enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable secret</td>
<td>Specifies an additional layer of security over the <strong>enable password</strong> command.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypts a password.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>more nvram:startup-config</td>
<td>Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.</td>
</tr>
<tr>
<td>privilege level</td>
<td>Sets the privilege level for the user.</td>
</tr>
</tbody>
</table>
enable secret

To specify an additional layer of security over the enable password command, use the enable secret command in global configuration mode. To turn off the enable secret function, use the no form of this command.

enable secret [level level] {[0] unencrypted-password | encryption-type encrypted-password}
no enable secret [level level] [encryption-type encrypted-password]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level level</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>unencrypted-password</td>
</tr>
<tr>
<td>encryption-type</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>encrypted-password</td>
</tr>
</tbody>
</table>

Command Default

No password is defined.

Command Modes

Global configuration (config)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If neither the enable password command or the enable secret command is configured, and if a line password is configured for the console, the console line password serves as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.
Use the `enable secret` command to provide an additional layer of security over the `enable password` password. The `enable secret` command provides better security by storing the password using a nonreversible cryptographic function. The additional layer of security encryption is useful in environments where the password is sent to the network or is stored on a TFTP server.

Typically, you enter an encryption type only when you paste an encrypted password that you copied from a device configuration file, into this command.

**Caution**

If you specify an encryption type and then enter a cleartext password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted earlier.

If you use the same password for the `enable password` and `enable secret` commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the `enable secret` command provides.

**Note**

After you set a password using the `enable secret` command, a password set using the `enable password` command works only if the `enable secret` is disabled. Additionally, you cannot recover a lost password that has been encrypted by any method.

If the `service password-encryption` command is set, the encrypted form of the password you create is displayed when the `more nvram:startup-config` command is run.

You can enable or disable password encryption with the `service password-encryption` command.

An enable password is defined as follows:

- Must contain a combination of numerals from 1 to 25, and uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combination Ctrl-v when you create the password; for example, to create the password `abc?123`, do the following:
  1. Enter `abc`.
  2. Press `Ctrl-v`.
  3. Enter `?123`.

**Note**

When the system prompts you to enter the `enable password` command, you need not precede the question mark with `Ctrl-v`; you can enter `abc?123` at the password prompt.

**Examples**

The following example shows how to specify a password with the `enable secret` command:

```
Device> enable
Device# configure terminal
```
Device(config)# enable secret password

After specifying a password with the enable secret command, users must enter this password to gain access. Otherwise, passwords set using the enable password command will no longer work.

Password: password

The following example shows how to enable the encrypted password $1$FaD0$Xyti5Rkls3LoyxzS8, which has been copied from a device configuration file, for privilege level 2, using the encryption type 4:

Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8

The following example shows the warning message that is displayed when a user enters the enable secret 4 encrypted-password command:

Device> enable
Device# configure terminal
Device(config)# enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been deprecated. Migrate to a supported password type

Device(config)# end
Device# show running-config | inc secret
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable password</td>
<td>Sets a local password to control access to various privilege levels.</td>
</tr>
<tr>
<td>more nvram:startup-config</td>
<td>Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.</td>
</tr>
<tr>
<td>service password-encryption</td>
<td>Encrypt passwords.</td>
</tr>
</tbody>
</table>
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 (config)

**Command History**

```
Release     Modification
Cisco IOS XE Everest 16.5.1a  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` command.

This example shows how to configure an open directive.

```
Device> enable
Device# configure terminal
Device(config)# epm access-control open
Device(config)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Displays the contents of the current running configuration file.</td>
</tr>
</tbody>
</table>
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
- **access-list-name**: Name of the security group access control list (SGACL).

### Command Default
Role-based ACLs are not configured.

### Command Modes
Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list role-based rbacl1
Device(config-rb-acl)# permit ip log
Device(config-rb-acl)# end
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit ip log</td>
<td>Permits logging that matches the configured entry.</td>
</tr>
<tr>
<td>show ip access-list</td>
<td>Displays contents of all current IP access lists.</td>
</tr>
</tbody>
</table>
ip admission

To enable web authentication, use the ip admission command in interface configuration mode or 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 (config-if)
- Fallback-profile configuration (config-fallback-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `ip admission` command applies a web authentication rule to a switch port.

This example shows how to apply a web authentication rule to a switchport:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip admission rule1
Device(config-if)# end
```

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> enable
Device# configure terminal
Device(config)# fallback profile profile1
Device(config-fallback-profile)# ip admission rule1
Device(config-fallback-profile)# end
```
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**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Name of network admission control rule.</td>
</tr>
<tr>
<td><code>consent</code></td>
<td>Associates an authentication proxy consent web page with the IP admission rule specified using the admission-name argument.</td>
</tr>
<tr>
<td><code>proxy http</code></td>
<td>Configures web authentication custom page.</td>
</tr>
<tr>
<td><code>absolute-timer minutes</code></td>
<td>(Optional) Elapsed time, in minutes, before the external server times out.</td>
</tr>
<tr>
<td><code>inactivity-time minutes</code></td>
<td>(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.</td>
</tr>
<tr>
<td>`list acl</td>
<td>acl-name</td>
</tr>
<tr>
<td><code>service-policy type tag service-policy-name</code></td>
<td>(Optional) A control plane service policy is to be configured.</td>
</tr>
</tbody>
</table>

**Command Default**

Web authentication is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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> enable
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> enable
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**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x fallback</td>
<td>Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.</td>
</tr>
<tr>
<td>fallback profile</td>
<td>Creates a web authentication fallback profile.</td>
</tr>
<tr>
<td>ip admission</td>
<td>Enables web authentication on a port.</td>
</tr>
<tr>
<td>show authentication sessions interface interface detail</td>
<td>Displays information about the web authentication session status.</td>
</tr>
<tr>
<td>show ip admission</td>
<td>Displays information about NAC cached entries or the NAC configuration.</td>
</tr>
</tbody>
</table>
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.

```
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.
The DHCP-snooping database is not configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2
Device(config)# exit
```

This example shows how to specify the amount of time before writing DHCP snooping entries to an external server:

```
evice> enable
Device# configure terminal
Device(config)# ip dhcp snooping database write-delay 15
Device(config)# exit
```
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 device 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 device hostname as the remote ID.
- **string string** Specify a remote ID, using from 1 to 63 ASCII characters (no spaces).

**Command Default**
The device MAC address is the remote ID.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 device MAC address. This command allows you to configure either the device 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> enable
Device# configure terminal
Device(config)# ip dhcp snooping information option format remote-id hostname
Device(config)# exit
```
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 (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
By default, the DHCP snooping feature verifies that the relay-agent IP address (giaddr) field in DHCP client message on an untrusted port is 0; the message is dropped if the giaddr field is not 0. Use the `ip dhcp snooping verify no-relay-agent-address` command to disable the verification. Use the `no ip dhcp snooping verify no-relay-agent-address` to reenable verification.

This example shows how to enable verification of the giaddr in a DHCP client message:

```
Device> enable
Device# configure terminal
Device(config)# no ip dhcp snooping verify no-relay-agent-address
Device(config)# exit
```
**ip http access-class**

To specify the access list that should be used to restrict access to the HTTP server, use the `ip http access-class` command in global configuration mode. To remove a previously configured access list association, use the `no` form of this command.

```
ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } | ipv6 access-list-name }
no ip http access-class { access-list-number | ipv4 { access-list-number | access-list-name } | ipv6 access-list-name }
```

**Syntax Description**

- `access-list-number`: Standard IP access list number in the range 0 to 99, as configured by the `access-list` global configuration command.
- `ipv4`: Specifies the IPv4 access list to restrict access to the secure HTTP server.
- `access-list-name`: Name of a standard IPv4 access list, as configured by the `ip access-list` command.
- `ipv6`: Specifies the IPv6 access list to restrict access to the secure HTTP server.

**Command Default**

No access list is applied to the HTTP server.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
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
Device(config-std-nacl)# exit
```

The following example shows how to define an IPv4 named access list as and assign it to the HTTP server.

```
Device> enable
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
Device(config)# exit

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list</td>
<td>Assigns an ID to an access list and enters access list configuration mode.</td>
</tr>
<tr>
<td>ip http server</td>
<td>Enables the HTTP 1.1 server, including the Cisco web browser user interface.</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>Name of the interface that RADIUS uses for all of its outgoing packets.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Per virtual route forwarding (VRF) configuration.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 disjoined 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**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>Binding MAC address.</td>
</tr>
<tr>
<td>vlan  vlan-id</td>
<td>Specifies the Layer 2 VLAN identification; valid values are from 1 to 4094.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Binding IP address.</td>
</tr>
<tr>
<td>interface  interface-id</td>
<td>ID of the physical interface.</td>
</tr>
</tbody>
</table>

**Command Default**

No IP source bindings are configured.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config) ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1
Device(config)# exit
```
ip ssh source-interface

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the `ip ssh source-interface` command in global configuration mode. To remove the IP address as the source address, use the `no` form of this command.

```
ip ssh source-interface interface
no ip ssh source-interface interface
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>The interface whose address is used as the source address for the SSH client.</td>
</tr>
</tbody>
</table>

**Command Default**

The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

**Examples**

In the following example, the IP address assigned to GigabitEthernet interface 1/0/1 is used as the source address for the SSH client:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh source-interface GigabitEthernet 1/0/1
Device(config)# exit
```
**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.

```plaintext
ip verify source [mac-check][tracking]
nopip verify source
```

| mac-check | (Optional) Enables IP source guard with MAC address verification. |
| tracking  | (Optional) Enables IP port security to learn static IP address learning on a port. |

**Command Default**
IP source guard is disabled.

**Command Modes**
Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```plaintext
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source
Device(config-if)# end
```

This example shows how to enable IP source guard with MAC address verification:

```plaintext
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip verify source mac-check
Device(config-if)# end
```

You can verify your settings by entering the `show ip verify source` 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
no ipv6 access-list access-list-name | client permit-control-packets | log-update threshold | role-based list-name
```

### Syntax Description

- **ipv6 access-list** `access-list-name`:
  - Creates a named IPv6 ACL (up to 64 characters in length) and enters IPv6 ACL configuration mode.
  - `access-list-name`: Name of the IPv6 access list. Names cannot contain a space or quotation mark, or begin with a numeric.

- **match-local-traffic**:
  - Enables matching for locally-generated traffic.

- **log-update threshold** `threshold-in-msgs`:
  - Determines how syslog messages are generated after the initial packet match.
  - `threshold-in-msgs`: Number of packets generated.

- **role-based** `list-name`:
  - Creates a role-based IPv6 ACL.

### Command Default

No IPv6 access list is defined.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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. 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> enable
Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# end
```

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 from GigabitEthernet interface 0/1/2. 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> enable
Device# configure terminal
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 gigabitethernet 0/1/2
Device(config-if)# ipv6 traffic-filter list2 out
Device(config-if)# end
```
ipv6 snooping 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 (config)

**Command History**
- **Modification**
  - 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> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# end
```
**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.

```plaintext
key chain name macsec
no key chain name [macsec]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Name of a key chain to be used to get keys.</td>
</tr>
</tbody>
</table>

**Command Default**

Key chain macsec is disabled.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure MACsec key chain to fetch a 128-bit Pre Shared Key (PSK):

```plaintext
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 1000
Device(config-keychain-macsec)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-macsec-key)# key-string fb63e0269e2768c49bab8ee9a5c2258f
Device(config-keychain-macsec-key)# end
Device#
```

This example shows how to configure MACsec key chain to fetch a 256-bit Pre Shared Key (PSK):

```plaintext
Device> enable
Device# configure terminal
Device(config)# key chain kc1 macsec
Device(config-keychain-macsec)# key 2000
Device(config-keychain-macsec)# cryptographic-algorithm aes-256-cmac
Device(config-keychain-macsec-key)# key-string c865632acb26902247c417504a1b
Device(config-keychain-macsec-key)# end
Device#
```
key config-key password-encrypt

To store a type 6 encryption key in private NVRAM, use the `key config-key password-encrypt` command in global configuration mode. To disable the encryption, use the `no` form of this command.

```
key config-key password-encrypt [text]
no key config-key password-encrypt [text]
```

**Syntax Description**

- `text` (Optional) Password or master key.

**Note**

We recommended that you do not use the `text` argument, and instead use interactive mode (using the `Enter` key after you enter the `key config-key password-encrypt` command) so that the preshared key is not printed anywhere and, therefore, cannot be seen.

**Command Default**

Type 6 password encryption key is not stored in private NVRAM.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can securely store plain text passwords in type 6 format in NVRAM using a CLI. Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the `key config-key password-encrypt` command along with the `password encryption aes` command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the `key config-key password-encrypt` command is the master encryption key that is used to encrypt all other keys in the device.

If you configure the `password encryption aes` command without configuring the `key config-key password-encrypt` command, the following message is displayed at startup or during a nonvolatile generation (NVGEN) process, such as when the `show running-config` or `copy running-config startup-config` commands are configured:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

**Changing a Password**

If the password (master key) is changed or reencrypted, use the `key config-key password-encrypt` command for the list registry to pass the old key and the new key to the application modules that are using type 6 encryption.

**Deleting a Password**

If the master key that was configured using the `key config-key password-encrypt` command is deleted from the system, a warning is displayed (and a confirm prompt is issued) stating that all type 6 passwords will become useless. As a security measure, after the passwords are encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be re-encrypted, as explained in the previous paragraph.
If the password that is configured using the `key config-key password-encrypt` command is lost, it cannot be recovered. We, therefore, recommend that you store the password in a safe location.

**Caution**

Unconfiguring Password Encryption

If you unconfigure password encryption using the `no password encryption aes` command, all the existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the `key config-key password-encrypt` command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can read the password (configured using the `key config-key password-encrypt` command), there is no way that the password can be retrieved from the device. Existing management stations cannot know what it is unless the stations are enhanced to include this key somewhere, in which case, the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a device. Before or after the configurations are loaded onto a device, the password must be manually added (using the `key config-key password-encrypt` command). The password can be manually added to the stored configuration. However we do not recommend this because adding the password manually allows anyone to decrypt all the passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste ciphertext that does not match the master key, or if there is no master key, the ciphertext is accepted or saved, but an alert message is displayed:

```
"ciphertext>[for username bar]> is incompatible with the configured master key."
```

If a new master key is configured, all plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or is unknown, you have the option of deleting the master key using the `no key config-key password-encrypt` command. Deleting the master key causes the existing encrypted passwords to remain encrypted in the device configuration. The passwords cannot be decrypted.

**Examples**

The following example shows how a type 6 encryption key is stored in NVRAM:

```
Device> enable
Device# configure terminal
Device (config)# key config-key password-encrypt
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password encryption aes</td>
<td>Enables a type 6 encrypted preshared key.</td>
</tr>
</tbody>
</table>
limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the `limit address-count` command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode or IPv6 snooping configuration mode. To return to the default, use the `no` form of this command.

```
limit address-count maximum
no limit address-count
```

**Syntax Description**

`maximum`  The number of addresses allowed on the port. The range is from 1 to 10000.

**Command Default**

The default is no limit.

**Command Modes**

- IPv6 snooping configuration (config-ipv6-snooping)
- ND inspection policy configuration (config-nd-inspection)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy policy1
Device(config-nd-inspection)# limit address-count 25
Device(config-nd-inspection)# end
```

This example shows how to define an IPv6 snooping policy name as policy1, and limit the number of IPv6 addresses allowed on the port to 25:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# limit address-count 25
Device(config-ipv6-snooping)# end
```
mab logging verbose

To filter detailed information from MAC authentication bypass (MAB) system messages, use the `mab logging verbose` command in global configuration mode. Use the `no` form of this command to disable logging MAB system messages.

```
mab logging verbose
no mab logging verbose
```

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

**Command Default**
Detailed logging of system messages is not enabled.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# mab logging verbose
Device(config)# exit
```

You can verify your settings by entering the `show running-config` command.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authentication logging verbose</td>
<td>Filters details from authentication system messages.</td>
</tr>
<tr>
<td>dot1x logging verbose</td>
<td>Filters details from 802.1x system messages.</td>
</tr>
<tr>
<td>mab logging verbose</td>
<td>Filters details from MAC authentication bypass (MAB) system messages.</td>
</tr>
</tbody>
</table>
mab request format attribute 32

To enable VLAN ID-based MAC authentication on a device, 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 (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 device:

```
Device> enable
Device# configure terminal
Device(config)# mab request format attribute 32 vlan access-vlan
Device(config)# exit
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>authentication event</code></td>
<td>Sets the action for specific authentication events.</td>
</tr>
<tr>
<td><code>authentication fallback</code></td>
<td>Configures a port to use web authentication as a fallback method for clients that do not support IEEE 802.1x authentication.</td>
</tr>
<tr>
<td><code>authentication host-mode</code></td>
<td>Sets the authorization manager mode on a port.</td>
</tr>
<tr>
<td><code>authentication open</code></td>
<td>Enables or disables open access on a port.</td>
</tr>
<tr>
<td><code>authentication order</code></td>
<td>Sets the order of authentication methods used on a port.</td>
</tr>
<tr>
<td><code>authentication periodic</code></td>
<td>Enables or disables reauthentication on a port.</td>
</tr>
<tr>
<td><code>authentication port-control</code></td>
<td>Enables manual control of the port authorization state.</td>
</tr>
<tr>
<td><code>authentication priority</code></td>
<td>Adds an authentication method to the port-priority list.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>authentication timer</strong></td>
<td>Configures the timeout and reauthentication parameters for an 802.1x-enabled port.</td>
</tr>
<tr>
<td><strong>authentication violation</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>mab</strong></td>
<td>Enables MAC-based authentication on a port.</td>
</tr>
<tr>
<td><strong>mab eap</strong></td>
<td>Configures a port to use the Extensible Authentication Protocol (EAP).</td>
</tr>
<tr>
<td><strong>show authentication</strong></td>
<td>Displays information about authentication manager events on the device.</td>
</tr>
</tbody>
</table>
**macsec network-link**

To enable MACsec Key Agreement protocol (MKA) configuration on the uplink interfaces, use the `macsec network-link` command in interface configuration mode. To disable it, use the `no` form of this command.

```
macsec network-link
no 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 (config-if)

**Command History**

- **Release**
  - Cisco IOS XE Everest 16.5.1a

- **Modification**
  - This command was introduced.

This example shows how to configure MACsec MKA on an interface using the EAP-TLS authentication protocol:

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/20
Device(config-if)# macsec network-link
Device(config-if)# end
Device#
```
**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. To remove the match parameters, use the `no` form of this command.

```
macth {ip address {namenumber} [{namenumber}] [{namenumber}] ... | ipv6 address {namenumber} [{namenumber}] [{namenumber}] ... | mac address {name} [{name}] [{name}] ...}

nomacth {ip address {namenumber} [{namenumber}] [{namenumber}] ... | ipv6 address {namenumber} [{namenumber}] [{namenumber}] ... | 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.
- `name` Name of the access list to match packets against.
- `number` Number of the access list to match packets against. This option is not valid for MAC access lists.

**Command Default**

The default action is to have no match parameters applied to a VLAN map.

**Command Modes**

Access-map configuration (config-access-map)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
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
Device(config)# exit

You can verify your settings by entering the `show vlan access-map` command.
# mka pre-shared-key

To configure MACsec Key Agreement (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 interface configuration mode. To disable it, use the `no` form of this command.

### Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mka pre-shared-key key-chain</td>
<td>Enables MACsec MKA configuration on device interfaces using a PSK.</td>
</tr>
<tr>
<td>no mka pre-shared-key key-chain</td>
<td>Disables MACsec MKA configuration on device interfaces.</td>
</tr>
</tbody>
</table>

### Command Default

MKA pre-shared-key is disabled.

### Command Modes

Interface configuration (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to configure MKA MACsec on an interface using a PSK:

```
Device> enable
Device# configure terminal
Device(config)# interface Gigabitethernet 1/0/20
Device(config-if)# mka pre-shared-key key-chain kcl
Device(config-if)# end
Device#
```
mka suppress syslogs sak-rekey

To suppress MACsec Key Agreement (MKA) secure association key (SAK) rekey messages during logging, use the `mka suppress syslogs sak-rekey` command in global configuration mode. To enable MKA SAK rekey message logging, use the `no` form of this command.

```
mka suppress syslogs sak-rekey
no mka suppress syslogs sak-rekey
```

This command has no arguments or keywords.

**Command Default**
All MKA SAK syslog messages are displayed on the console.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
MKA SAK syslogs are continuously generated at every rekey interval, and when MKA is configured on multiple interfaces, the amount of syslog generated is too high. Use this command to suppress the MKA SAK syslogs.

**Example**
The following example shows how to suppress MKA SAK syslog logging:

```
Device> enable
Device# configure terminal
Device(config)# mka suppress syslogs sak-rekey
```
password encryption aes

To enable a type 6 encrypted preshared key, use the `password encryption aes` command in global configuration mode. To disable password encryption, use the `no` form of this command.

```
password encryption aes
no password encryption aes
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Preshared keys are not encrypted.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can securely store plain text passwords in type 6 format in NVRAM using a CLI. Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the `key config-key password-encrypt` command along with the `password encryption aes` command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) that is configured using the `key config-key password-encrypt` command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the `password encryption aes` command without configuring the `key config-key password-encrypt` command, the following message is displayed at startup or during a nonvolatile generation (NVGEN) process, such as when the `show running-config` or `copy running-config startup-config` commands are run:

```
"Can not encrypt password. Please configure a configuration-key with 'key config-key'"
```

**Changing a Password**

If the password (master key) is changed or re-encrypted using the `key config-key password-encrypt` command, the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

**Deleting a Password**

If the master key that was configured using the `key config-key password-encrypt` command is deleted from the system, a warning is displayed (and a confirm prompt is issued) that states that all type 6 passwords will no longer be applicable. As a security measure, after the passwords are encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be re-encrypted as explained in the previous paragraph.

**Caution**

If a password that is configured using the `key config-key password-encrypt` command is lost, it cannot be recovered. Therefore, the password should be stored in a safe location.

**Unconfiguring Password Encryption**
If you unconfigure password encryption using the `no password encryption aes` command, all the existing type 6 passwords are left unchanged. As long as the password (master key) that was configured using the `key config-key password-encrypt` command exists, the type 6 passwords are decrypted as and when required by the application.

**Storing Passwords**

Because no one can read the password (configured using the `key config-key password-encrypt` command), there is no way that the password can be retrieved from the router. Existing management stations cannot know what it is unless the stations are enhanced to include this key somewhere. Therefore, the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the `key config-key password-encrypt` command). The password can be manually added to the stored configuration, but we do not recommend this because adding the password manually allows anyone to decrypt all the passwords in that configuration.

**Configuring New or Unknown Passwords**

If you enter or cut and paste ciphertext that does not match the master key, or if there is no master key, the ciphertext is accepted or saved, but the following alert message is displayed:

```
ciphertext>[for username bar>] is incompatible with the configured master key.```

If a new master key is configured, all the plain keys are encrypted and converted to type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the `no key config-key password-encrypt` command. This causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

**Examples**

The following example shows how a type 6 encrypted preshared key is enabled:

```
Device> enable
Device# configure terminal
Device (config)# password encryption aes
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>key config-key password-encrypt</td>
<td>Stores a type 6 encryption key in private NVRAM.</td>
</tr>
</tbody>
</table>
permit (MAC access-list configuration)

To allow non-IP traffic to be forwarded if the conditions are matched, use the `permit` command in MAC access-list configuration mode. To remove a permit condition from the extended MAC access list, use the `no` form of this command.

```plaintext
permit {any | host src-MAC-addr | src-MAC-addr mask} {any | host dst-MAC-addr | dst-MAC-addr mask} {type mask | aarp | amber | appletalk | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | lsap lsap mask | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp} [cos cos]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>any</code></td>
<td>Denies any source or destination MAC address.</td>
</tr>
<tr>
<td>`host src-MAC-addr</td>
<td>src-MAC-addr mask`</td>
</tr>
<tr>
<td>`host dst-MAC-addr</td>
<td>dst-MAC-addr mask`</td>
</tr>
</tbody>
</table>
| `type mask` | (Optional) Specifies the EtherType number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.  
  - `type` is 0 to 65535, specified in hexadecimal.  
  - `mask` is a mask of don’t care bits applied to the EtherType before testing for a match. |
| `aarp` | (Optional) Specifies EtherType AppleTalk Address Resolution Protocol that maps a data-link address to a network address. |
| `amber` | (Optional) Specifies EtherType DEC-Amber. |
| `appletalk` | (Optional) Specifies EtherType AppleTalk/EtherTalk. |
| `dec-spanning` | (Optional) Specifies EtherType Digital Equipment Corporation (DEC) spanning tree. |
| `decnet-iv` | (Optional) Specifies EtherType DECnet Phase IV protocol. |
| `diagnostic` | (Optional) Specifies EtherType DEC-Diagnostic. |
permit (MAC access-list configuration)

- **dsm**
  *(Optional) Specifies EtherType DEC-DSM.*

- **etype-6000**
  *(Optional) Specifies EtherType 0x6000.*

- **etype-8042**
  *(Optional) Specifies EtherType 0x8042.*

- **lat**
  *(Optional) Specifies EtherType DEC-LAT.*

- **lavc-sca**
  *(Optional) Specifies EtherType DEC-LAVC-SCA.*

- **lsap lsap-number mask**
  *(Optional) Specifies the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.
  
The *mask* is a mask of don’t care bits applied to the LSAP number before testing for a match.

- **mop-console**
  *(Optional) Specifies EtherType DEC-MOP Remote Console.*

- **mop-dump**
  *(Optional) Specifies EtherType DEC-MOP Dump.*

- **msdos**
  *(Optional) Specifies EtherType DEC-MSDOS.*

- **mumps**
  *(Optional) Specifies EtherType DEC-MUMPS.*

- **netbios**
  *(Optional) Specifies EtherType DEC- Network Basic Input/Output System (NetBIOS).*

- **vines-echo**
  *(Optional) Specifies EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems.*

- **vines-ip**
  *(Optional) Specifies EtherType VINES IP.*

- **xns-idp**
  *(Optional) Specifies EtherType Xerox Network Systems (XNS) protocol suite.*

- **cos cos**
  *(Optional) Specifies an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the *cos* option is configured.*

---

**Command Default**

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

**Command Modes**

MAC-access list configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 XE terminology are listed in the following table.

<table>
<thead>
<tr>
<th>IPX Encapsulation Type</th>
<th>Novell Name</th>
<th>Filter Criterion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>arpa</td>
<td>Ethernet II</td>
<td>EtherType 0x8137</td>
</tr>
<tr>
<td>snap</td>
<td>Ethernet-snap</td>
<td>EtherType 0x8137</td>
</tr>
<tr>
<td>sap</td>
<td>Ethernet 802.2</td>
<td>LSAP 0xE0E0</td>
</tr>
<tr>
<td>novell-ether</td>
<td>Ethernet 802.3</td>
<td>LSAP 0xFFFF</td>
</tr>
</tbody>
</table>

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> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
Device(config-ext-macl)# end
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
Device(config-ext-macl)# end
```

This example permits all packets with EtherType 0x4321:

```
Device> enable
Device# configure terminal
Device(config)# mac access-list extended
Device(config-ext-macl)# permit any any 0x4321 0
Device(config-ext-macl)# end
```

You can verify your settings by entering the `show access-lists` command.
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>deny</strong></td>
<td>Denies from the MAC access-list configuration. Denies non-IP traffic to be forwarded if conditions are matched.</td>
</tr>
<tr>
<td><strong>mac access-list extended</strong></td>
<td>Creates an access list based on MAC addresses for non-IP traffic.</td>
</tr>
<tr>
<td><strong>show access-lists</strong></td>
<td>Displays access control lists configured on a device.</td>
</tr>
</tbody>
</table>
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 in IPv6 snooping configuration mode. 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 (config-ipv6-snooping)

**Command History**

- **Release**: Cisco IOS XE Everest 16.5.1a
- **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`, and configure the port to use DHCP to glean addresses:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# protocol dhcp
Device(config-ipv6-snooping)# end
```
To configure the RADIUS server parameters, including the RADIUS accounting and authentication, use the `radius server` command in global configuration mode. 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**

<table>
<thead>
<tr>
<th>Address</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`ip{address</td>
<td>hostname}`</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>auth-port udp-port</code></td>
<td>(Optional) Specifies the UDP port for the RADIUS authentication server. The range is from 0 to 65536.</td>
</tr>
<tr>
<td><code>acct-port udp-port</code></td>
<td>(Optional) Specifies the UDP port for the RADIUS accounting server. The range is from 0 to 65536.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>key string</code></td>
<td>(Optional) Specifies the authentication and encryption key for all RADIUS communication between the device and the RADIUS daemon.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>automate tester  name</code></td>
<td>(Optional) Enables automatic server testing of the RADIUS server status, and specify the username to be used.</td>
</tr>
<tr>
<td><code>retransmit  value</code></td>
<td>(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.</td>
</tr>
<tr>
<td><code>timeout seconds</code></td>
<td>(Optional) Specifies the time interval that the device 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 command.</td>
</tr>
</tbody>
</table>

**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**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` command in RADIUS server configuration mode. 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> enable
Device# configure terminal
Device(config)# radius server ISE
Device(config-radius-server)# address ipv4 10.1.1 auth-port 1645 acct-port 1646
Device(config-radius-server)# key cisco123
Device(config-radius-server)# end
```
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 (config-ipv6-snooping)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to define an IPv6 snooping policy name as policy1 and configure the security level as inspect:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# security-level inspect
Device(config-ipv6-snooping)# end
```
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ip-address</code></td>
<td>IP address of the IPsec gateway that is terminating the VPN tunnel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>wlan</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to modify IPSec pass-through.

```
Device> enable
Device# configure terminal
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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>IP address of the private RADIUS server host.</td>
</tr>
<tr>
<td>auth-port</td>
<td>(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.</td>
</tr>
<tr>
<td>acct-port</td>
<td>Optional) UDP destination port for accounting requests. The default value is 1646.</td>
</tr>
<tr>
<td>non-standard</td>
<td>(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.</td>
</tr>
<tr>
<td>timeout</td>
<td>(Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the <code>radius-server timeout</code> command. If no timeout value is specified, the global value is used.</td>
</tr>
<tr>
<td>retransmit</td>
<td>(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 <code>radius-server retransmit</code> command.</td>
</tr>
<tr>
<td>key</td>
<td>(Optional) Authentication and encryption key used between the device and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the <code>radius-server key</code> command. If no key string is specified, the global value is used. The <code>string</code> 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.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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
Device(config-sg-radius)# end
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>aaa group server</code></td>
<td>Groups different server hosts into distinct lists and distinct methods.</td>
</tr>
<tr>
<td><code>aaa new-model</code></td>
<td>Enables the AAA access control model.</td>
</tr>
<tr>
<td><code>password encryption aes</code></td>
<td>Enables a type 6 encrypted preshared key.</td>
</tr>
<tr>
<td><code>radius-server host</code></td>
<td>Specifies a RADIUS server host.</td>
</tr>
<tr>
<td><code>radius-server directed-request</code></td>
<td>Allows users to log in to a Cisco NAS and select a RADIUS server for authentication.</td>
</tr>
</tbody>
</table>
show aaa clients

To display authentication, authorization, and accounting (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 (>)
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show aaa clients` command:

```
Device> enable
Device# show aaa clients

Dropped request packets: 0
```
show aaa command handler

To display authentication, authorization, and accounting (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 (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show aaa command handler` command:

```
Device# show aaa command handler

AAA Command Handler Statistics:
  account-logon: 0, account-logoff: 0
  account-query: 0, pod: 0
  service-logon: 0, service-logoff: 0
  user-profile-push: 0, session-state-log: 0
  reauthenticate: 0, bounce-host-port: 0
  disable-host-port: 0, update-rbacl: 0
  update-sgt: 0, update-cts-policies: 0
  invalid commands: 0
  async message not sent: 0
```
show aaa local

To display authentication, authorization, and accounting (AAA) local method options, use the `show aaa local` command.

```
show aaa local { netuser { name | all } | statistics | user lockout }
```

**Syntax Description**

- `netuser` Specifies the AAA local network or guest user database.
- `name` Network user name.
- `all` Specifies the network and guest user information.
- `statistics` Displays statistics for local authentication.
- `user lockout` Specifies the AAA local locked-out user.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show aaa local statistics` command:

```
Device# show aaa local statistics

Local EAP statistics

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Success</th>
<th>Fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAP-MD5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>LEAP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PEAP</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAP-MSCCHAPV2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

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
```
show aaa servers

To display all authentication, authorization, and accounting (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 (>)
- Privileged EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

The following is a sample 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 display authentication, authorization, and accounting (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 (>
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample 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 brief

To display brief information about authentication sessions for a given interface, use the `show authentication brief` command in either user EXEC or privileged EXEC mode.

```
show authentication brief[switch{switch-number|active|standby}{R0}]
```

**Syntax Description**

| switch-number | Valid values for the `switch-number` variable are from 1 to 9. |
| R0            | Displays information about the Route Processor (RP) slot 0. |
| active        | Specifies the active instance. |
| standby       | Specifies the standby instance. |

**Command Modes**

- Privileged EXEC (#)
- User EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show authentication brief` command:

```
Device# show authentication brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>AuthC</th>
<th>AuthZ</th>
<th>Fg</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0001 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>281s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0002 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>280s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0003 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>279s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0004 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>278s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0005 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>278s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0006 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>277s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0007 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>276s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0008 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>276s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0009 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>275s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000a m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>275s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000b m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>274s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000c m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>274s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000d m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>273s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000e m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>273s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.000f m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>272s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0010 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>272s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0011 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>271s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0012 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>271s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0013 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>270s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0014 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>270s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0015 m:NA d:OK</td>
<td>A2: SA-</td>
<td></td>
<td>X</td>
<td>269s</td>
</tr>
</tbody>
</table>
```

The following is a sample output from the `show authentication brief` command for active instances:
Device# `show authentication brief switch active R0`

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>AuthC</th>
<th>AuthZ</th>
<th>Fg</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0001</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>1s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0002</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>0s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0003</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>299s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0004</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>298s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0005</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>298s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0006</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>297s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0007</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>296s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0008</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>296s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0009</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>295s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0010</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>294s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0000</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>294s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0002</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>293s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0003</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>292s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0004</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>292s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0005</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>291s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0006</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>291s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0007</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>290s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0008</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>289s</td>
</tr>
<tr>
<td>Gi2/0/14</td>
<td>0002.0002.0009</td>
<td>m:NA d:OK</td>
<td>AZ: SA-</td>
<td>X</td>
<td>289s</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show authentication brief` command for standby instances:

Device# `show authentication brief switch standby R0`

No sessions currently exist

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

**Table 158: show authentication brief Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The type and number of the authentication interface.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the client.</td>
</tr>
<tr>
<td>AuthC</td>
<td>Indicates authentication status.</td>
</tr>
<tr>
<td>AuthZ</td>
<td>Indicates authorization status.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Fg    | Flag indicates the current status. The valid values are:  
  • A—Applying policy (multi-line status for details)  
  • D—Awaiting removal  
  • F—Final removal in progress  
  • I—Awaiting IIF ID allocation  
  • P—Pushed session  
  • R—Removing user profile (multi-line status for details)  
  • U—Applying user profile (multi-line status for details)  
  • X—Unknown blocker |
| Uptime| Indicates the duration since which the session came up |
**show authentication history**

To display the authenticated sessions alive on a device, use the `show authentication history` command in user EXEC or privileged EXEC mode.

```
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 (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `show authentication history` command to display the authenticated sessions alive on the device.

The following is sample output from the `show authentication history` command:

```
Device# show authentication history

Interface    MAC Address  Method   Domain  Status  Uptime
Gi3/0/2      0021.d864.07c0 dot1x  DATA    Auth    38s

Session count = 1
```
show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command.

```
show authentication sessions [ database ] [ handle handle-id [ details ] ] [ interface type number [ details ] ] [ mac mac-address [ interface type number ] [ method method-name [ interface type number [ details ] ] ] ] [ session-id session-id [ details ] ]
```

**Syntax Description**

- **database** (Optional) Shows only data stored in session database.
- **handle handle-id** (Optional) Specifies the particular handle for which Auth Manager information is to be displayed.
- **details** (Optional) Shows detailed information.
- **interface type number** (Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed.
- **mac mac-address** (Optional) Specifies the particular MAC address for which you want to display information.
- **method method-name** (Optional) Specifies the particular authentication method for which Auth Manager information is to be displayed. If you specify a method (dot1x, mab, or webauth), you may also specify an interface.

**Command Modes**

User EXEC (>)

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 159: Authentication Method States

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not run</td>
<td>The method has not run for this session.</td>
</tr>
<tr>
<td>Running</td>
<td>The method is running for this session.</td>
</tr>
<tr>
<td>Failed over</td>
<td>The method has failed and the next method is expected to provide a result.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success</td>
<td>The method has provided a successful authentication result for the session.</td>
</tr>
<tr>
<td>Authc Failed</td>
<td>The method has provided a failed authentication result for the session.</td>
</tr>
</tbody>
</table>

**Table 160: Authentication Method States**

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>802.1X</td>
</tr>
<tr>
<td>mab</td>
<td>MAC authentication bypass</td>
</tr>
<tr>
<td>webauth</td>
<td>web authentication</td>
</tr>
</tbody>
</table>

The following example shows how to display all authentication sessions on the device:

Device# `show authentication sessions`

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Method</th>
<th>Domain</th>
<th>Status</th>
<th>Session ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/48</td>
<td>0015.63b0.f676</td>
<td>dot1x</td>
<td>DATA</td>
<td>Authz Success</td>
<td>0A3462B1000000102983C05C</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>000f.23c4.a401</td>
<td>mab</td>
<td>DATA</td>
<td>Authz Success</td>
<td>0A3462B10000000D4F80B58</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0014.bf5d.d26d</td>
<td>dot1x</td>
<td>DATA</td>
<td>Authz Success</td>
<td>0A3462B10000000E29811B94</td>
</tr>
</tbody>
</table>

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
```

This command reference is from Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches).
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 cisp

To display Client Information Signaling Protocol (CISP) information for a specified interface, use the show cisp command in privileged EXEC mode.

```plaintext
show cisp { [clients | interface interface-id] | registrations | summary}
```

### Syntax Description

- **clients**
  - (Optional) Display CISP client details.

- **interface interface-id**
  - (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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show cisp interface` command:

```plaintext
Device# show cisp interface fastethernet 0/1/1
CISP not enabled on specified interface
```

The following is sample output from the `show cisp registrations` command:

```plaintext
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   Auth Mgr  (Authenticator)
Gi3/0/5   Auth Mgr  (Authenticator)
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisp enable</td>
<td>Enables CISP.</td>
</tr>
<tr>
<td>dot1x credentials $profile</td>
<td>Configures a profile on a supplicant device.</td>
</tr>
</tbody>
</table>
show dot1x

To display IEEE 802.1x statistics, administrative status, and operational status for a device or for the specified port, use the `show dot1x` command in user EXEC or privileged 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 (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show dot1x all` command:

```
Device# show dot1x all
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

The following is sample 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
```

The following is sample output from the `show dot1x all statistics` command:

```
Device# show dot1x statistics
```
Dot1x Global Statistics for
--------------------------------------------
<table>
<thead>
<tr>
<th>RxStart</th>
<th>RxLogoff</th>
<th>RxResp</th>
<th>RxRespID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>RxReq</th>
<th>RxInvalid</th>
<th>RxLenErr</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

| RxTotal | |
|---------| |
| 0       | |

<table>
<thead>
<tr>
<th>TxStart</th>
<th>TxLogoff</th>
<th>TxResp</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TxReq</th>
<th>ReTxReq</th>
<th>ReTxReqFail</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TxReqID</th>
<th>ReTxReqID</th>
<th>ReTxReqIDFail</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TxTotal</th>
<th>TxStart</th>
<th>TxLogoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TxTotal</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
</tr>
</tbody>
</table>
**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show eap pac peers` command:

```
Device# show eap pac peers
No PACs stored
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear eap sessions</td>
<td>Clears EAP session information for the device or for the specified port.</td>
</tr>
</tbody>
</table>
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 or privileged EXEC mode.

```
show ip dhcp snooping statistics  [detail ]
```

**Syntax Description**

- `detail` (Optional) Displays detailed statistics information.

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

```
Release          Modification
Cisco IOS XE Everest 16.5.1a  This command was introduced.
```

**Usage Guidelines**

In a device stack, all statistics are generated on the stack master. If a new active device is elected, the statistics counters reset.

The following is sample 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
```

The following is sample 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>
<thead>
<tr>
<th>DHCP Snooping Statistic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Processed by DHCP Snooping</td>
<td>Total number of packets handled by DHCP snooping, including forwarded and dropped packets.</td>
</tr>
<tr>
<td>Packets Dropped Because IDB not known</td>
<td>Number of errors when the input interface of the packet cannot be determined.</td>
</tr>
<tr>
<td>Queue full</td>
<td>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.</td>
</tr>
<tr>
<td>Interface is in errdisabled</td>
<td>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.</td>
</tr>
<tr>
<td>Rate limit exceeded</td>
<td>Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state.</td>
</tr>
<tr>
<td>Received on untrusted ports</td>
<td>Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped.</td>
</tr>
<tr>
<td>Nonzero giaddr</td>
<td>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.</td>
</tr>
<tr>
<td>Source mac not equal to chaddr</td>
<td>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.</td>
</tr>
<tr>
<td>Binding mismatch</td>
<td>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 device 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.</td>
</tr>
<tr>
<td>Insertion of opt82 fail</td>
<td>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.</td>
</tr>
</tbody>
</table>
### DHCP Snooping Statistic

<table>
<thead>
<tr>
<th>Description</th>
<th>DHCP Snooping Statistic</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td>Interface Down</td>
</tr>
<tr>
<td>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.</td>
<td>Unknown output interface</td>
</tr>
<tr>
<td>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.</td>
<td>Reply output port equal to input port</td>
</tr>
<tr>
<td>Number of times the packet has been denied by a platform-specific registry.</td>
<td>Packet denied by platform</td>
</tr>
</tbody>
</table>
show radius server-group

To display properties for the RADIUS server group, use the `show radius server-group` command in user EXEC or privileged EXEC mode.

```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

The following is sample 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 162: show radius server-group command Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server group</td>
<td>Name of the server group.</td>
</tr>
<tr>
<td>Sharecount</td>
<td>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.</td>
</tr>
<tr>
<td>sg_unconfigured</td>
<td>Server group has been unconfigured.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Type</td>
<td>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 &quot;nonstandard&quot;.</td>
</tr>
<tr>
<td>Memlocks</td>
<td>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.</td>
</tr>
</tbody>
</table>
show storm-control

To display broadcast, multicast, or unicast storm control settings on the device or on the specified interface or to display storm-control history, use the **show storm-control** command in user EXEC or privileged EXEC mode.

**show storm-control [interface-id] [broadcast | multicast | unicast]**

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-id</td>
<td>(Optional) Interface ID for the physical port (including type, stack member for stacking-capable devices, module, and port number).</td>
</tr>
<tr>
<td>broadcast</td>
<td>(Optional) Displays broadcast storm threshold setting.</td>
</tr>
<tr>
<td>multicast</td>
<td>(Optional) Displays multicast storm threshold setting.</td>
</tr>
<tr>
<td>unicast</td>
<td>(Optional) Displays unicast storm threshold setting.</td>
</tr>
</tbody>
</table>

**Command Modes**

User EXEC (>)

Privileged EXEC (>)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 device. If you do not enter a traffic type, settings appear for broadcast storm control.

The following is sample 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

<table>
<thead>
<tr>
<th>Interface</th>
<th>Filter State</th>
<th>Upper</th>
<th>Lower</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>Forwarding</td>
<td>20 pps</td>
<td>10 pps</td>
<td>5 pps</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>Forwarding</td>
<td>50.00%</td>
<td>40.00%</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The following table describes the fields in the show storm-control display:
Table 163: show storm-control Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Displays the ID of the interface.</td>
</tr>
<tr>
<td>Filter State</td>
<td>Displays the status of the filter:</td>
</tr>
<tr>
<td></td>
<td>• Blocking—Storm control is enabled, and a storm has occurred.</td>
</tr>
<tr>
<td></td>
<td>• Forwarding—Storm control is enabled, and no storms have occurred.</td>
</tr>
<tr>
<td></td>
<td>• Inactive—Storm control is disabled.</td>
</tr>
<tr>
<td>Upper</td>
<td>Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second.</td>
</tr>
<tr>
<td>Lower</td>
<td>Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second.</td>
</tr>
<tr>
<td>Current</td>
<td>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.</td>
</tr>
</tbody>
</table>
show tech-support acl

To display access control list (ACL)-related information for technical support, use the `show tech-support acl` command in privileged EXEC mode.

```
show tech-support acl
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of the `show tech-support acl` command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support acl | redirect flash:show_tech_acl.txt`) in the local writable storage file system or remote file system.

The output of this command displays the following commands:

```
• show clock
• show version
• show running-config
• show module
• show interface
• show access-lists
• show logging
• show platform software fed switch switch-number acl counters hardware
• show platform software fed switch switch-number ifm mapping
• show platform hardware fed switch switch-number fwd-asic drops exceptions
• show platform software fed switch switch-number acl info
```

**Note**

On stackable platforms, these commands are executed on every switch in the stack. On modular platforms, like Catalyst 9400 Series Switches, these commands are run only on the active switch.

**Note**

The following list of commands is a sample of the commands available in the output; these may differ based on the platform.
The following is sample output from the `show tech-support acl` command:

```
Device# show tech-support acl
.
.
------------------ show platform software fed switch 1 acl cam brief ------------------

Printing entries for region ACL_CONTROL (143) type 6 asic 0
 ==============================================================
TAQ-4 Index-0 (A:0,C:0) Valid StartF-1 StartA-1 SkipF-0 SkipA-0
Output IPv4 VACL

VCU Result: Not In-Use

L3 Length: 0000, L3 Protocol: 17 (UDP), L3 Tos: 00
Source Address/Mask
0.0.0.0/0.0.0.0
```
Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
show tech-support acl

L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00
Source Address/Mask 0.0.0.0/0.0.0.0
Destination Address/Mask 0.0.0.0/0.0.0.0
Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled
L4 Source Port/Mask L4 Destination Port/Mask 0x0000 (0)/0x0000 0x0000 (0)/0x0000
TCP Flags: 0x00 ( NOT SET )
ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----------------------------------------
TAQ-4 Index-4 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output IPv4 PACL
VCU Result: Not In-Use
L3 Length: 0000, L3 Protocol: 00 (HOPOPT), L3 Tos: 00
Source Address/Mask 0.0.0.0/0.0.0.0
Destination Address/Mask 0.0.0.0/0.0.0.0
Router MAC: Disabled, Not First Fragment: Disabled, Small Offset: Disabled
L4 Source Port/Mask L4 Destination Port/Mask 0x0000 (0)/0x0000 0x0000 (0)/0x0000
TCP Flags: 0x00 ( NOT SET )
ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

-----------------------------------------
TAQ-4 Index-5 (A:0,C:0) Valid StartF-0 StartA-0 SkipF-0 SkipA-0
Output MAC PACL
VLAN ID/MASK : 0x000 (000)/0x000
Source MAC/Mask : 0000.0000.0000/0000.0000.0000
Destination MAC/Mask : 0000.0000.0000/0000.0000.0000
isSnap: Disabled, isLLC: Disabled
ACTIONS: Drop L3, Drop L2, Logging Disabled
ACL Priority: 2 (15 is Highest Priority)

Output fields are self-explanatory.
**show tech-support identity**

To display identity/802.1x-related information for technical support, use the **show tech-support identity** command in privileged EXEC mode.

```
show tech-support identity mac mac-address interface interface-name
```

**Syntax Description**
- `mac mac-address` Displays information about the client MAC address.
- `interface interface-name` Displays information about the client interface.

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of the **show tech-support platform** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support identity mac mac-address interface interface-name | redirect flash:filename**) in the local writable storage file system or remote file system.

The output of this command displays the following commands:

- `show clock`
- `show module`
- `show version`
- `show switch`
- `show redundancy`
- `show dot1x statistics`
- `show ip access-lists`
- `show interface`
- `show ip interface brief`
- `show vlan brief`
- `show running-config`
- `show logging`
- `show interface controller`
- `show platform authentication sbinfo interface`
• show platform host-access-table
• show platform pm port-data
• show spanning-tree interface
• show access-session mac detail
• show platform authentication session mac
• show device-tracking database mac details
• show mac address-table address
• show access-session event-logging mac
• show authentication sessions mac details R0
• show ip admission cache R0
• show platform software wired-client R0
• show platform software wired-client F0
• show platform software process database forwarding-manager R0 summary
• show platform software process database forwarding-manager F0 summary
• show platform software object-manager F0 pending-ack-update
• show platform software object-manager F0 pending-issue-update
• show platform software object-manager F0 error-object
• show platform software peer forwarding-manager R0
• show platform software peer forwarding-manager F0
• show platform software VP R0 summary
• show platform software VP F0 summary
• show platform software fed punt cpuq
• show platform software fed punt cause summary
• show platform software fed inject cause summary
• show platform hardware fed fwd-asic drops exceptions
• show platform hardware fed fwd-asic resource tcam table acl
• show platform software fed acl counter hardware
• show platform software fed matm macTable
• show platform software fed ifm mappings
• show platform software trace message fed reverse
• show platform software trace message forwarding-manager R0 reverse
• show platform software trace message forwarding-manager F0 reverse
- show platform software trace message smd R0 reverse
- show authentication sessions mac details
- show platform software wired-client
- show platform software process database forwarding-manager summary
- show platform software object-manager pending-ack-update
- show platform software object-manager pending-issue-update
- show platform software object-manager error-object
- show platform software peer forwarding-manager
- show platform software VP summary
- show platform software trace message forwarding-manager reverse
- show ip admission cache
- show platform software trace message smd reverse
- show platform software fed punt cpuq
- show platform software fed punt cause summary
- show platform software fed inject cause summary
- show platform hardware fed fwd-asic drops exceptions
- show platform hardware fed fwd-asic resource team table acl
- show platform software fed acl counter hardware
- show platform software fed matm macTable
- show platform software fed ifm mappings
- show platform software trace message fed reverse

Examples

The following is sample output from the **show tech-support identity** command:

```
Device# show tech-support identity mac 0000.0001.0003 interface gigabitethernet1/0/1
.
.
------------------ show platform software peer forwarding-manager R0 ------------------
IOSD Connection Information:
MQIPC (reader) Connection State: Connected, Read-selected
  Connections: 1, Failures: 22
  3897 packet received (0 dropped), 466929 bytes
  Read attempts: 2352, Yields: 0
BIPC Connection state: Connected, Ready
  Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
  36 packets sent, 2808 bytes

SMD Connection Information:
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 30
0 packet received (0 dropped), 0 bytes
Read attempts: 1, Yields: 0
MQIPC (writer) Connection State: Connected, Ready
Connections: 1, Failures: 0, Backpressures: 0
0 packet sent, 0 bytes

FP Peers Information:

Slot: 0
Peer state: connected
OM ID: 0, Download attempts: 638
Complete: 638, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 1
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
Tx Packets: 688, Messages: 2392, ACKs: 36
Rx Packets: 37, Bytes: 2068

IPC Log:
Peer name: fman-log-bay0-peer0
Flags: Recovery-Complete
Send Seq: 36, Recv Seq: 36, Mags Sent: 0, Mags Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdff3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdff3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdff40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdff4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCGRD IPC Context:
State: Connected
BIPC Handle: 0xdff41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
  State: Connected
  BIPC Handle: 0xdfe440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
  CM ID: 1, Download attempts: 1
    Complete: 1, Yields: 0, Spurious: 0
    IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
  Back-Pressure asserted for IPC: 0, IPC-Log: 0
  Number of FP FMAN peer connection expected: 7
  Number of FP FMAN online msg received: 1
  IPC state: unknown

Config IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdfe54e4d8, BIPC FD: 48, Peer Context: 0xdfe70e18
  Tx Packets: 20, Messages: 704, ACKs: 1
  Rx Packets: 2, Bytes: 108
  IPC Log:
    Peer name: fman-log-bay0-peer1
    Flags: Recovery-Complete
    Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdfe70fe8, BIPC FD: 49, Peer Context: 0xdfe70e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0

Upstream FMRP-IOsd IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdfe863f8, BIPC FD: 50, Peer Context: 0xdfe70e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-SMD IPC Context:
  State: Connected, Read-selected
  BIPC Handle: 0xdf962228, BIPC FD: 51, Peer Context: 0xdf970e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
  State: Connected
  BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf970e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
  State: Connected
  BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf970e18
  TX Packets: 0, Bytes: 0, Drops: 0
  Rx Packets: 0, Bytes: 0
  Rx ACK Requests: 0, Tx ACK Responses: 0
Upstream FMRP-MOBILITYD IPC Context:
State: Connected
BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

------------------ show platform software peer forwarding-manager R0 ------------------

IOSD Connection Information:
MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 22
3897 packet received (0 dropped), 466929 bytes
Read attempts: 2352, Yields: 0
BIPC Connection state: Connected, Ready
Accepted: 1, Rejected: 0, Closed: 0, Backpressures: 0
36 packets sent, 2808 bytes

SMD Connection Information:
MQIPC (reader) Connection State: Connected, Read-selected
Connections: 1, Failures: 30
0 packet received (0 dropped), 0 bytes
Read attempts: 1, Yields: 0
MQIPC (writer) Connection State: Connected, Ready
Connections: 1, Failures: 0, Backpressures: 0
0 packet sent, 0 bytes

FP Peers Information:
Slot: 0
Peer state: connected
OM ID: 0, Download attempts: 638
Complete: 638, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 1
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3d48e8, BIPC FD: 36, Peer Context: 0xdf3e7158
Tx Packets: 688, Messages: 2392, ACKs: 36
Rx Packets: 37, Bytes: 2068

IPC Log:
Peer name: fman-log-bay0-peer0
Flags: Recovery-Complete
Send Seq: 36,Recv Seq: 36,Msgs Sent: 0,Msgs Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3e7308, BIPC FD: 37, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf3f9c38, BIPC FD: 38, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 37, Bytes: 2864
Rx ACK Requests: 1, Tx ACK Responses: 1

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf40c568, BIPC FD: 39, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdf4317c8, BIPC FD: 41, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
State: Connected
BIPC Handle: 0xdf41ee98, BIPC FD: 40, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
State: Connected
BIPC Handle: 0xdf4440f8, BIPC FD: 42, Peer Context: 0xdf3e7158
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Slot: 1
Peer state: connected
OM ID: 1, Download attempts: 1
Complete: 1, Yields: 0, Spurious: 0
IPC Back-Pressure: 0, IPC-Log Back-Pressure: 0
Back-Pressure asserted for IPC: 0, IPC-Log: 0
Number of FP FMAN peer connection expected: 7
Number of FP FMAN online msg received: 1
IPC state: unknown

Config IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf45e4d8, BIPC FD: 48, Peer Context: 0xdf470e18
TX Packets: 20, Messages: 704, ACKs: 1
Rx Packets: 2, Bytes: 108

IPC Log:
Peer name: fman-log-bay0-peer1
Flags: Recovery-Complete
Send Seq: 1, Recv Seq: 1, Msgs Sent: 0, Msgs Recovered: 0

Upstream FMRP IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf470fc8, BIPC FD: 49, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0

Upstream FMRP-IOSd IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf4838f8, BIPC FD: 50, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-SMD IPC Context:
State: Connected, Read-selected
BIPC Handle: 0xdf496228, BIPC FD: 51, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCD_0 IPC Context:
State: Connected
BIPC Handle: 0xdf4bb488, BIPC FD: 53, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-WNCMGRD IPC Context:
State: Connected
BIPC Handle: 0xdf4a8b58, BIPC FD: 52, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

Upstream FMRP-MOBILITYD IPC Context:
State: Connected
BIPC Handle: 0xdf4cddb8, BIPC FD: 54, Peer Context: 0xdf470e18
TX Packets: 0, Bytes: 0, Drops: 0
Rx Packets: 0, Bytes: 0
Rx ACK Requests: 0, Tx ACK Responses: 0

-------------------- show platform software VP R0 summary ------------------

Forwarding Manager Vlan Port Information

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Intf-ID</th>
<th>Stp-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>27</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>28</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>29</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>30</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>31</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>40</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>41</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>

Forwarding Manager Vlan Port Information

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Intf-ID</th>
<th>Stp-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>49</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>51</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>63</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>72</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>73</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>74</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>
### Forwarding Manager Vlan Port Information

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Intf-ID</th>
<th>Stp-state</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>9</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>17</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>27</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>28</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>29</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>30</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>31</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>40</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>41</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>49</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>51</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>63</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>72</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>73</td>
<td>Forwarding</td>
</tr>
<tr>
<td>1</td>
<td>74</td>
<td>Forwarding</td>
</tr>
</tbody>
</table>

---

### Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)

- `show tech-support identity`
show vlan access-map

To display information about a particular VLAN access map or for all VLAN access maps, use the **show vlan access-map** command in privileged EXEC mode.

```
show vlan access-map [map-name]
```

**Syntax Description**

- **map-name** (Optional) Name of a specific VLAN access map.

**Command Modes**

- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the **show vlan access-map** command:

```
Device# show vlan access-map

Vlan access-map "vmap4" 10
  Match clauses:
    ip address: al2
  Action:
    forward
Vlan access-map "vmap4" 20
  Match clauses:
    ip address: al2
  Action:
    forward
```
show vlan filter

To display information about all VLAN filters or about a particular VLAN or VLAN access map, use the show vlan filter command in privileged EXEC mode.

```
show vlan filter {access-map name | vlan vlan-id}
```

**Syntax Description**
- **access-map name** (Optional) Displays filtering information for the specified VLAN access map.
- **vlan vlan-id** (Optional) Displays filtering information for the specified VLAN. The range is 1 to 4094.

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the show vlan filter command:

```
Device# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```
show vlan group

To display the VLANs that are mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

```
show vlan group [[group-name vlan-group-name [user_count]]]
```

**Syntax Description**

- **group-name** vlan-group-name (Optional) Displays the VLANs mapped to the specified VLAN group.
- **user_count** (Optional) Displays the number of users in each VLAN mapped to a specified VLAN group.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>5</td>
</tr>
<tr>
<td>41</td>
<td>8</td>
</tr>
<tr>
<td>42</td>
<td>12</td>
</tr>
<tr>
<td>43</td>
<td>2</td>
</tr>
<tr>
<td>44</td>
<td>9</td>
</tr>
<tr>
<td>45</td>
<td>0</td>
</tr>
</tbody>
</table>
```
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 | unknown-unicast} level {level {level-low} | bps bps [bps-low] | pps pps [pps-low]}}
no storm-control {action {shutdown | trap} | {broadcast | multicast | unicast | unknown-unicast} level}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>shutdown</strong></td>
<td>Disables the port during a storm.</td>
</tr>
<tr>
<td><strong>trap</strong></td>
<td>Sends an SNMP trap when a storm occurs.</td>
</tr>
<tr>
<td><strong>broadcast</strong></td>
<td>Enables broadcast storm control on the interface.</td>
</tr>
<tr>
<td><strong>multicast</strong></td>
<td>Enables multicast storm control on the interface.</td>
</tr>
<tr>
<td><strong>unicast</strong></td>
<td>Enables unicast storm control on the interface.</td>
</tr>
<tr>
<td><strong>unknown-unicast</strong></td>
<td>Enables unknown unicast storm control on an interface.</td>
</tr>
<tr>
<td><strong>level</strong></td>
<td>Specifies the rising and falling suppression levels as a percentage of total bandwidth of the port.</td>
</tr>
<tr>
<td><strong>level-low</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>bps</strong></td>
<td>Specifies the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.</td>
</tr>
<tr>
<td><strong>bps-low</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>pps</strong></td>
<td>Specifies the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.</td>
</tr>
<tr>
<td><strong>pps-low</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>Command Default</strong></td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>Broadcast, multicast, and unicast storm control are disabled. The default action is to filter traffic and to not send an SNMP trap.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command Modes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface configuration (config-if)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Usage Guidelines</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked. However, the device 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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>traps and shutdown options</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The trap and shutdown options are independent of each other.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>traps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>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 device generates a trap when a storm is detected).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>shutdown</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the device blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the device blocks traffic until the traffic rate drops below this level.</td>
</tr>
</tbody>
</table>
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.

Note

When a broadcast storm occurs and the action is to filter traffic, the device 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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# storm-control broadcast level 75.5
Device(config-if)# end
```

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# storm-control unicast level 87 65
Device(config-if)# end
```

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> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# storm-control multicast level pps 2k 1k
Device(config-if)# end
```

This example shows how to enable the `shutdown` action on a port:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# storm-control action shutdown
Device(config-if)# end
```

You can verify your settings by entering the `show storm-control` command.
switchport port-security aging

To set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port, use the `switchport port-security aging` command in interface configuration mode. To disable port security aging or to set the parameters to their default states, use the `no` form of this command.

```
switchport port-security aging {static | time time | type {absolute | inactivity}}
no switchport port-security aging {static | time | type}
```

**Syntax Description**

- **static**: Enables aging for statically configured secure addresses on this port.
- **time time**: Specifies the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port.
- **type**: Sets the aging type.
  - **absolute**: Sets absolute aging type. All the secure addresses on this port age out exactly after the time (minutes) specified and are removed from the secure address list.
  - **inactivity**: Sets the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

**Command Default**

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# switchport port-security aging time 120
```
Device(config-if)# end

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port:

Device> enable
Device# configure terminal
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
Device(config-if)# end

This example shows how to disable aging for configured secure addresses:

Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet1/0/2
Device(config-if)# no switchport port-security aging static
Device(config-if)# end
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
no switchport port-security mac-address {mac-address [{vlan {vlan-id {access | voice}}}]} | sticky
```

### 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 (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 device 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` command.

This example shows how to configure a secure MAC address and a VLAN ID on a port:

```
Device> enable
Device# configure terminal
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
Device(config-if)# end
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Device> enable
Device# configure terminal
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
Device(config-if) # end
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.

**Syntax**

```
switchport port-security maximum value [vlan [vlan-list | {access | voice}]]
no switchport port-security maximum value [vlan [vlan-list | {access | voice}]]
```

**Syntax Description**

- **value** (Optional) 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 (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The maximum number of secure MAC addresses that you can configure on a device 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; 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.
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` 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> enable
Device# configure terminal
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
Device(config-if)# end
```
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 (config-if)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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; 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.

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 shows how to configure a port to shut down only the VLAN if a MAC security violation occurs:

```
Device> enable
Device# configure terminal
Device(config)# interface gigabitethernet2/0/2
Device(config)# switchport port-security violation shutdown vlan
Device(config)# exit
```
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>address ipv6 (TACACS+)</code></td>
<td>Configures the IPv6 address of the TACACS+ server.</td>
</tr>
<tr>
<td><code>key (TACACS+)</code></td>
<td>Configures the per-server encryption key on the TACACS+ server.</td>
</tr>
<tr>
<td><code>port (TACACS+)</code></td>
<td>Specifies the TCP port to be used for TACACS+ connections.</td>
</tr>
<tr>
<td><code>send-nat-address (TACACS+)</code></td>
<td>Sends a client’s post-NAT address to the TACACS+ server.</td>
</tr>
<tr>
<td><code>single-connection (TACACS+)</code></td>
<td>Enables all TACACS packets to be sent to the same server using a single TCP connection.</td>
</tr>
<tr>
<td><code>timeout(TACACS+)</code></td>
<td>Configures the time to wait for a reply from the specified TACACS server.</td>
</tr>
</tbody>
</table>
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 }] }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>enable</th>
<th>Enables tracking.</th>
</tr>
</thead>
<tbody>
<tr>
<td>reachable-lifetime</td>
<td>(Optional) Specifies the maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The reachable-lifetime keyword can be used only with the enable keyword.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use of the reachable-lifetime keyword overrides the global reachable lifetime configured by the ipv6 neighbor binding reachable-lifetime command.</td>
<td></td>
</tr>
<tr>
<td>value</td>
<td>Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.</td>
<td></td>
</tr>
<tr>
<td>infinite</td>
<td>Keeps an entry in a reachable or stale state for an infinite amount of time.</td>
<td></td>
</tr>
<tr>
<td>disable</td>
<td>Disables tracking.</td>
<td></td>
</tr>
<tr>
<td>stale-lifetime</td>
<td>(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The stale lifetime is 86,400 seconds.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The stale-lifetime keyword can be used only with the disable keyword.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use of the stale-lifetime keyword overrides the global stale lifetime configured by the ipv6 neighbor binding stale-lifetime command.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**
The time entry is kept in a reachable state.

**Command Modes**
IPv6 snooping configuration (config-ipv6-snooping)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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 and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# tracking disable stale-lifetime infinite
Device(config-ipv6-snooping)# end
```
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 (config-nd-inspection)
IPv6 snooping configuration (config-ipv6-snooping)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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, and configures the port to be trusted:

Device> enable
Device# configure terminal
Device(config)# ipv6 nd inspection policy1
Device(config-nd-inspection)# trusted-port
Device(config-nd-inspection)# end

This example shows how to define an IPv6 snooping policy name as policy1, and configures the port to be trusted:

Device> enable
Device# configure terminal
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# trusted-port
Device(config-ipv6-snooping)# end
username

To establish the username-based authentication system, use the `username` command in global configuration mode. To remove an established username-based authentication, use the `no` form of this command.

```
username name [aaa attribute list aaa-list-name]
username name [access-class access-list-number]
username name [algorithm-type {md5 | scrypt | sha256}]
username name [autocommand command]
username name [callback-dialstring telephone-number]
username name [callback-line [tty] line-number [ending-line-number]]
username name [callback-rotary rotary-group-number]
username name [common-criteria-policy policy-name]
username name [dnis]
username name [mac]
username name [nocallback-verify]
username name [noescape]
username name [nohangup]
username name [{nopassword | password password | password encryption-type encrypted-password}]
username name [one-time {password {0 | 6 | 7} password} | secret {0 | 5 | 8 | 9} password}]
username name [password secret]
username name [privilege level]
username name [secret {0 | 5} password]
username name [serial-number]
username name [user-maxlinks number]
username name [view view-name]
no username name
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Hostname, server name, user ID, or command name. The <code>name</code> argument can be only one word. Blank spaces and quotation marks are not allowed.</td>
</tr>
<tr>
<td><code>aaa attribute list</code></td>
<td>(Optional) Uses the specified authentication, authorization, and accounting (AAA) method list.</td>
</tr>
<tr>
<td><code>aaa-list-name</code></td>
<td></td>
</tr>
<tr>
<td><code>access-class</code></td>
<td>(Optional) Specifies an outgoing access list that overrides the access list specified in the <code>access-class</code> command that is available in line configuration mode. It is used for the duration of the user’s session.</td>
</tr>
<tr>
<td><code>access-list-number</code></td>
<td></td>
</tr>
<tr>
<td><code>algorithm-type</code></td>
<td>(Optional) Specifies the algorithm to use for hashing the plaintext secret for the user.</td>
</tr>
</tbody>
</table>

- **md5**: Encodes the password using the MD5 algorithm.
- **scrypt**: Encodes the password using the SCRYPT hashing algorithm.
- **sha256**: Encodes the password using the PBKDF2 hashing algorithm.
### autocommand command
(Optional) Causes the specified `autocommand` command to be issued automatically after the user logs in. When the specified `autocommand` command is complete, the session is terminated. Because the command can be of any length and can contain embedded spaces, commands using the `autocommand` keyword must be the last option on the line.

### callback-dialstring
**telephone-number**
(Optional) Permits you to specify a telephone number to pass to the Data Circuit-terminating Equipment (DCE) device; for asynchronous callback only.

### callback-line
**line-number**
(Optional) Specifies relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback; for asynchronous callback only. Numbering begins with zero.

### ending-line-number
(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as `tty`), then line number and ending line number are absolute rather than relative line numbers.

### tty
(Optional) Specifies standard asynchronous line; for asynchronous callback only.

### callback-rotary
**rotary-group-number**
(Optional) Permits you to specify a rotary group number on which you want to enable a specific username for callback; for asynchronous callback only. The next available line in the rotary group is selected. Range: 1 to 100.

### common-criteria-policy
(Optional) Specifies the name of the common criteria policy.

### dnis
(Optional) Does not require a password when obtained through the Dialed Number Identification Service (DNIS).

### mac
(Optional) Allows a MAC address to be used as the username for MAC filtering done locally.

### nocallback-verify
(Optional) Specifies that authentication is not required for EXEC callback on the specified line.

### noescape
(Optional) Prevents the user from using an escape character on the host to which that user is connected.

### nohangup
(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the `autocommand` keyword) is run. Instead, the user gets another user EXEC prompt.

### nopassword
(Optional) No password is required for the user to log in. This is usually the most useful keyword to use in combination with the `autocommand` keyword.

### password
(Optional) Specifies a password to access the `name` argument. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the `username` command.

### password
Password that the user enters.
**Encryption-type**

Single-digit number that defines whether the text immediately following the **password** is encrypted, and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following the **password** is not encrypted, and 6 and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.

<table>
<thead>
<tr>
<th>encryption-type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Specifies that an unencrypted password or secret (depending on the configuration) follows.</td>
</tr>
<tr>
<td>6</td>
<td>Specifies that an encrypt password follows.</td>
</tr>
<tr>
<td>7</td>
<td>Specifies that a hidden password follows.</td>
</tr>
<tr>
<td>5</td>
<td>Specifies that a MD5 HASHED secret follows.</td>
</tr>
<tr>
<td>8</td>
<td>Specifies that a PBKDF2 HASHED secret follows.</td>
</tr>
<tr>
<td>9</td>
<td>Specifies that a SCRYPT HASHED secret follows.</td>
</tr>
</tbody>
</table>

**Encrypted-password**

Encrypted password that the user enters.

**One-time**

(Optional) Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.

- **0**: Specifies that an unencrypted password or secret (depending on the configuration) follows.
- **6**: Specifies that an encrypt password follows.
- **7**: Specifies that a hidden password follows.
- **5**: Specifies that a MD5 HASHED secret follows.
- **8**: Specifies that a PBKDF2 HASHED secret follows.
- **9**: Specifies that a SCRYPT HASHED secret follows.

**Secret**

(Optional) Specifies a secret for the user.

**Secret**

For Challenge Handshake Authentication Protocol (CHAP) authentication. Specifies the secret for the local device or the remote device. The secret is encrypted when it is stored on the local device. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.

**Privilege privilege-level**

(Optional) Sets the privilege level for the user. Range: 1 to 15.

**Serial-number**

(Optional) Specifies the serial number.

**User-maxlinks number**

(Optional) Specifies the maximum number of inbound links allowed for the user.

**View view-name**

(Optional) Associates a CLI view name, which is specified with the parser view command, with the local AAA database; for CLI view only.

### Command Default

No username-based authentication system is established.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only. Multiple **username** commands can be used to specify options for a single user.
Add a username entry for each remote system with which the local device communicates, and from which it requires authentication. The remote device must have a username entry for the local device. This entry must have the same password as the local device’s entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an info username that does not require a password, but connects the user to a general purpose information service.

The `username` command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local device requires authentication.

To enable the local device to respond to remote CHAP challenges, one `username name` entry must be the same as the `hostname` entry that has already been assigned to the other device. To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1, for example, 0 or 2 through 15. Per-user privilege levels override virtual terminal privilege levels.

**CLI and Lawful Intercept Views**

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows the user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of SNMP commands that store information about calls and users.

Users who are specified via the `lawful-intercept` keyword are placed in the lawful-intercept view by default if no other privilege level or view name is explicitly specified.

If no value is specified for the `secret` argument, and the `debug serial-interface` command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the `debug ppp negotiation`, `debug serial-interface`, and `debug serial-packet` commands.

**Examples**

The following example shows how to implement a service similar to the UNIX `who` command, which can be entered at the login prompt, and lists the current users of the device:

```
Device> enable
Device# configure terminal
Device(config)# username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used:

```
Device> enable
Device# configure terminal
Device(config)# username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break:

```
Device> enable
Device# configure terminal
Device(config)# username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of `server_l`. It also defines a password for a remote server named `server_r`.

```
hostname server_l
username server_r password theirsystem
interface serial 0
```
encapsulation ppp
ppp authentication chap

The following is a sample output from the `show running-config` command displaying the passwords that are encrypted:

```
hostname server_l
username server_r password 7 121F0A18
interface serial 0
  encapsulation ppp
  ppp authentication chap
```

The following example shows how a privilege level 1 user is denied access to privilege levels higher than 1:

```
Device> enable
Device# configure terminal
Device(config)# username user privilege 0 password 0 cisco
Device(config)# username user2 privilege 2 password 0 cisco
```

The following example shows how to remove username-based authentication for user2:

```
Device> enable
Device# configure terminal
Device(config)# no username user2
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>debug ppp negotiation</code></td>
<td>Displays PPP packets sent during PPP startup, where PPP options are negotiated.</td>
</tr>
<tr>
<td><code>debug serial-interface</code></td>
<td>Displays information about a serial connection failure.</td>
</tr>
<tr>
<td><code>debug serial-packet</code></td>
<td>Displays more detailed serial interface debugging information than you can obtain using the <code>debug serial interface</code> command.</td>
</tr>
</tbody>
</table>
**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 device. To delete a VLAN map entry, use the `no` form of this command.

```
vlan access-map name [number]
no vlan access-map name [number]
```

**Syntax Description**

- `name` Name of the VLAN map.
- `number` (Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry.

**Command Default**

There are no VLAN map entries and no VLAN maps applied to a VLAN.

**Command Modes**

Global configuration (config)

**Command History**

- **Release** Cisco IOS XE Everest 16.5.1a
- **Modification** 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.

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> **enable**
Device# **configure terminal**
Device(config)# **vlan access-map vac1**
Device(config-access-map)# **match ip address acl1**
Device(config-access-map)# **action forward**
Device(config-access-map)# **end**

This example shows how to delete VLAN map vac1:

Device> **enable**
Device# **configure terminal**
Device(config)# **no vlan access-map vac1**
Device(config)# **exit**
To apply a VLAN map to one or more VLANs, use the `vlan filter` command in global configuration mode. Use the `no` form of this command to remove the map.

```
vlan filter mapname vlan-list {list | all}
no vlan filter mapname vlan-list {list | all}
```

**Syntax Description**
- `mapname` (required): Name of the VLAN map entry.
- `vlan-list` (required): Specifies which VLANs to apply the map to.
- `list` (optional): 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` (optional): Adds the map to all VLANs.

**Command Default**
There are no VLAN filters.

**Command Modes**
Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

This example applies VLAN map entry `map1` to VLANs 20 and 30:

```
Device> enable
Device# configure terminal
Device(config)# vlan filter map1 vlan-list 20, 30
Device(config)# exit
```

This example shows how to delete VLAN map entry `map1` from VLAN 20:

```
Device> enable
Device# configure terminal
Device(config)# no vlan filter map1 vlan-list 20
Device(config)# exit
```

You can verify your settings by entering the `show vlan filter` command.
vlan group

To create or modify a VLAN group, use the `vlan group` command in global configuration mode. To remove a VLAN list from the VLAN group, use the `no` form of this command.

```
vlan group group-name vlan-list vlan-list
no vlan group group-name vlan-list vlan-list
```

**Syntax Description**

- **group-name**
  Name of the VLAN group. The group name may contain up to 32 characters and must begin with a letter.

- **vlan-list**
  Specifies one or more VLANs to be added to the VLAN group. The `vlan-list` argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID range. Multiple entries are separated by a hyphen (-) or a comma (,).

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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> enable
Device# configure terminal
Device(config)# vlan group group1 vlan-list 7-9,11
Device(config)# exit
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Device> enable
Device# configure terminal
Device(config)# no vlan group group1 vlan-list 7
Device(config)# exit
```
PART XII

System Management

• System Management Commands, on page 1385
• Tracing, on page 1535
System Management Commands

- arp, on page 1387
- boot, on page 1388
- cat, on page 1389
- copy, on page 1390
- copy startup-config tftp:, on page 1391
- copy tftp: startup-config, on page 1392
- debug voice diagnostics mac-address, on page 1393
- debug platform condition feature multicast controlplane, on page 1394
- debug platform condition mac, on page 1396
- debug platform rep, on page 1397
- debug ilpower powerman, on page 1398
- delete, on page 1401
- dir, on page 1402
- emergency-install, on page 1404
- exit, on page 1406
- factory-reset, on page 1407
- flash_init, on page 1408
- help, on page 1409
- install, on page 1410
- l2 traceroute, on page 1414
- license boot level, on page 1415
- license smart deregister, on page 1417
- license smart register idtoken, on page 1418
- license smart renew, on page 1419
- location, on page 1420
- location plm calibrating, on page 1423
- mac address-table move update, on page 1424
- mgmt_init, on page 1425
- mkdir, on page 1426
- more, on page 1427
- no debug all, on page 1428
- rename, on page 1429
- request consent-token accept-response shell-access, on page 1430
• request consent-token generate-challenge shell-access, on page 1431
• request consent-token terminate-auth, on page 1432
• request platform software console attach switch, on page 1433
• reset, on page 1435
• rmdir, on page 1436
• sdm prefer, on page 1437
• service private-config-encryption, on page 1438
• set, on page 1439
• show avc client, on page 1442
• show debug, on page 1443
• show env, on page 1444
• show env xps, on page 1446
• show flow monitor, on page 1450
• show install, on page 1452
• show license all, on page 1454
• show license status, on page 1456
• show license summary, on page 1458
• show license udi, on page 1459
• show license usage, on page 1460
• show location, on page 1461
• show logging onboard switch uptime, on page 1463
• show mac address-table move update, on page 1466
• show parser encrypt file status, on page 1467
• show platform hardware fpga, on page 1468
• show platform integrity, on page 1469
• show platform software audit, on page 1470
• show platform software fed switch punt cause, on page 1474
• show platform software fed switch punt cpuq, on page 1476
• show platform sudi certificate, on page 1479
• show romvar, on page 1481
• show sdm prefer, on page 1482
• show tech-support license, on page 1484
• show tech-support platform, on page 1486
• show tech-support platform evpn_vxlan, on page 1490
• show tech-support platform fabric, on page 1492
• show tech-support platform igmp_snooping, on page 1496
• show tech-support platform layer3, on page 1499
• show tech-support platform mld_snooping, on page 1507
• show tech-support port, on page 1514
• show version, on page 1517
• system env temperature threshold yellow, on page 1524
• traceroute mac, on page 1526
• traceroute mac ip, on page 1529
• type, on page 1531
• unset, on page 1532
• version, on page 1534
To display the contents of the Address Resolution Protocol (ARP) table, use the `arp` command in boot loader mode.

```
arp [ip_address]
```

**Syntax Description**
- `ip_address` (Optional) Shows the ARP table or the mapping for a specific IP address.

**Command Default**
No default behavior or values.

**Command Modes**
Boot loader

**Command History**
- **Release**
  - Cisco IOS XE Everest 16.5.1a
  - 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.

- `filesystem:`  Alias for a file system. Use `flash:` for the system board flash device; use `usbflash0:` for USB memory sticks.

- `/file-url`  Path (directory) and name of a bootable image. Separate image names with a semicolon.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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:
**copy**

To copy a file from a source to a destination, use the `copy` command in boot loader mode.

`copy filesystem:/source-file-url filesystem:/destination-file-url`

**Syntax Description**

- `filesystem:` Alias for a file system. Use `usbflash0:` for USB memory sticks.
- `/source-file-url` Path (directory) and filename (source) to be copied.
- `/destination-file-url` Path (directory) and filename of the destination.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

| remote host [ip-address]/[name] | Host name or IP-address of Remote host. |

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 16.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

**Syntax Description**

```plaintext
copy tftp: startup-config remote host {ip-address}/{name}
```

- **remote host {ip-address}/{name}**: Host name or IP-address of Remote host.

**Command Default**

No default behavior or values.

**Command Modes**

- Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 16.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```plaintext
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
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>voice diagnostics</td>
<td>Configures voice debugging for voice clients.</td>
</tr>
<tr>
<td>mac-address mac-address1 mac-address mac-address2</td>
<td>Specifies MAC addresses of the voice clients.</td>
</tr>
<tr>
<td>verbose</td>
<td>Enables verbose mode for voice diagnostics.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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:

```plaintext
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```
debug platform condition feature multicast control plane

To enable radioactive tracing for the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping features, use the debug platform condition feature multicast control plane command in privileged EXEC mode. To disable radioactive tracing, use the no form of this command.

debug platform condition feature multicast control plane {{igmp-debug | pim} group-ip {ipv4 address | ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address | ipv6 address} vlan vlan-id} level {debug | error | info | verbose | warning}

no debug platform condition feature multicast control plane {{igmp-debug | pim} group-ip {ipv4 address | ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address | ipv6 address} vlan vlan-id} level {debug | error | info | verbose | warning}

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp-debug</td>
<td>Enables IGMP control radioactive tracing.</td>
</tr>
<tr>
<td>pim</td>
<td>Enables Protocol Independent Multicast (PIM) control radioactive tracing.</td>
</tr>
<tr>
<td>mld-snooping</td>
<td>Enables MLD snooping control radioactive tracing.</td>
</tr>
<tr>
<td>igmp-snooping</td>
<td>Enables IGMP snooping control radioactive tracing.</td>
</tr>
<tr>
<td>mac mac-address</td>
<td>MAC address of the receiver.</td>
</tr>
<tr>
<td>group-ip {ipv4 address</td>
<td>ipv6 address}</td>
</tr>
<tr>
<td>ip {ipv4 address</td>
<td>ipv6 address}</td>
</tr>
<tr>
<td>vlan vlan-id</td>
<td>VLAN ID. The range is from 1 to 4094.</td>
</tr>
<tr>
<td>level debug</td>
<td>Enables debug severity levels.</td>
</tr>
<tr>
<td>level error</td>
<td>Enables error debugging.</td>
</tr>
<tr>
<td>level info</td>
<td>Enables information debugging.</td>
</tr>
<tr>
<td>level verbose</td>
<td>Enables detailed debugging.</td>
</tr>
<tr>
<td>level warning</td>
<td>Enables warning debugging.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)
The following example shows how to enable radioactive tracing for IGMP snooping:

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac 000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear debug platform condition all</td>
<td>Removes the debug conditions applied to a platform.</td>
</tr>
<tr>
<td>debug platform condition</td>
<td>Filters debugging output for <code>debug</code> commands on the basis of specified conditions.</td>
</tr>
<tr>
<td>debug platform condition start</td>
<td>Starts conditional debugging on a system.</td>
</tr>
<tr>
<td>debug platform condition stop</td>
<td>Stops conditional debugging on a system.</td>
</tr>
<tr>
<td>show platform condition</td>
<td>Displays the currently active debug configuration.</td>
</tr>
</tbody>
</table>
**debug platform condition mac**

To enable radioactive tracing for MAC learning, use the `debug platform condition mac` command in privileged EXEC mode. To disable radioactive tracing for MAC learning, use the `no` form of this command.

```
deploy platform condition mac {mac-address {control-plane | egress | ingress} | access-list access-list name {egress | ingress}}
no debug platform condition mac {mac-address {control-plane | egress | ingress} | access-list access-list name {egress | ingress}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mac mac-address</code></td>
<td>Filters output on the basis of the specified MAC address.</td>
</tr>
<tr>
<td><code>access-list access-list name</code></td>
<td>Filters output on the basis of the specified access list.</td>
</tr>
<tr>
<td><code>control-plane</code></td>
<td>Displays messages about the control plane routines.</td>
</tr>
<tr>
<td><code>egress</code></td>
<td>Filters output on the basis of outgoing packets.</td>
</tr>
<tr>
<td><code>ingress</code></td>
<td>Filters output on the basis of incoming packets.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC (`#`)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows how to filter debugging output on the basis of a MAC address:

```
Device# debug platform condition mac bca6.6509.3314 ingress
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show platform condition</code></td>
<td>Displays the currently active debug configuration.</td>
</tr>
<tr>
<td><code>debug platform condition</code></td>
<td>Filters debugging output for <code>debug</code> commands on the basis of specified conditions.</td>
</tr>
<tr>
<td><code>debug platform condition start</code></td>
<td>Starts conditional debugging on a system.</td>
</tr>
<tr>
<td><code>debug platform condition stop</code></td>
<td>Stops conditional debugging on a system.</td>
</tr>
<tr>
<td><code>clear debug platform condition all</code></td>
<td>Removes the debug conditions applied to a platform.</td>
</tr>
</tbody>
</table>
debug platform rep

To enable debugging of Resilient Ethernet Protocol (REP) functions, use the `debug platform rep` command in privileged EXEC mode. To remove the specified condition, use the `no` form of this command.

```
debug platform rep {all | error | event | packet | verbose}
no debug platform rep {all | error | event | packet | verbose}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>all</code></td>
<td>Enables all REP debugging functions.</td>
</tr>
<tr>
<td><code>error</code></td>
<td>Enables REP error debugging.</td>
</tr>
<tr>
<td><code>event</code></td>
<td>Enables REP event debugging.</td>
</tr>
<tr>
<td><code>packet</code></td>
<td>Enables REP packet debugging.</td>
</tr>
<tr>
<td><code>verbose</code></td>
<td>Enables REP verbose debugging.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following example shows how to enable debugging for all functionss:

```
Device# debug platform rep all
debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show platform condition</td>
<td>Displays the currently active debug configuration.</td>
</tr>
<tr>
<td>debug platform condition</td>
<td>Filters debugging output for <code>debug</code> commands on the basis of specified conditions.</td>
</tr>
<tr>
<td>debug platform condition start</td>
<td>Starts conditional debugging on a system.</td>
</tr>
<tr>
<td>debug platform condition stop</td>
<td>Stops conditional debugging on a system.</td>
</tr>
<tr>
<td>clear debug platform condition all</td>
<td>Removes the debug conditions applied to a platform.</td>
</tr>
</tbody>
</table>
debug ilpower powerman

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the `debug ilpower powerman` command in privileged EXEC mode. Use the no form of this command to disable debugging.

**Command Default**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows the output for the `debug ilpower powerman` command for releases prior to Cisco IOS XE Gibraltar 16.10.1:

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface GiX/y/z: Power Controller reports power Imax error detected
   Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign is done by proto CDP
   Port Gi1/0/48: Selected Protocol CDP
   Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlv from cdp INPUT:
      Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
      power_man_id= 2,
      Mar 8 16:35:17.801: power_request_level[] = 2640 0 0 0 0
      Mar 8 16:35:17.801:
      Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) power negotiation:
         consumption = 2640, alloc_power= 2640
      Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold to 2640.
      Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
      Mar 8 16:35:18.115: ILP:: Gi1/0/48: State=NGWC_ILP_LINK_UP_S-6,
      Event=NGWC_ILP_IMAX_FAULT_EV-5
      Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdown Gi1/0/48
      Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48) delete allocated power 2640
      Mar 8 16:35:18.116: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold to 0.
      Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msg to slot:1 port:48
      Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlv Gi1/0/48 pwralloc0
      Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
      Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
```
This example shows the output for the `debug ilpower powerman` command starting Cisco IOS XE Gibraltar 16.10.1. Power Unit (mW) has been added to the power_request_level, PSE Allocation and PD Request. Power_request_level has been enhanced to display only non-zero values.

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlvfrom cdpINPUT:
Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1, power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<------------------------- mW unit added, non-zero value display
Mar 8 16:35:17.801: Mar 8 16:35:17.801: IILP:: Sending icutoffcurrent msg to slot:1 port:48
Mar 8 16:35:17.801:power_request_level(mW) = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold to 2640.
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power 2640
Mar 8 16:35:18.115: IILP:: Sending icutoffcurrent msg to slot:1 port:48
```

This example shows the output for the `debug ilpower powerman` command starting Cisco IOS XE Gibraltar 16.10.1. Power Unit (mW) has been added to the power_request_level, PSE Allocation and PD Request. Power_request_level has been enhanced to display only non-zero values.

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlv from cdp INPUT:
Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1, power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<------------------------- mW unit added, non-zero value display
Mar 8 16:35:17.801: Mar 8 16:35:17.801: IILP:: Sending icutoffcurrent msg to slot:1 port:48
Mar 8 16:35:17.801:power_request_level(mW) = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold to 2640.
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power 2640
Mar 8 16:35:18.115: IILP:: Sending icutoffcurrent msg to slot:1 port:48
```
debug ilpower powerman

(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prev) Power Pair : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:test5.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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 164: dir Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Index number of the file.</td>
</tr>
<tr>
<td>-rwx</td>
<td>File permission, which can be any or all of the following:</td>
</tr>
<tr>
<td></td>
<td>• d—directory</td>
</tr>
<tr>
<td></td>
<td>• r—readable</td>
</tr>
<tr>
<td></td>
<td>• w—writable</td>
</tr>
<tr>
<td></td>
<td>• x—executable</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>1644045</td>
<td>Size of the file.</td>
</tr>
<tr>
<td>&lt;date&gt;</td>
<td>Last modification date.</td>
</tr>
<tr>
<td>env_vars</td>
<td>Filename.</td>
</tr>
</tbody>
</table>
To perform an emergency installation on your system, use the `emergency-install` command in boot loader mode.

This feature is not supported on the Cisco Catalyst 9500 Series High Performance Switches.

**Syntax Description**

```
emergency-install url://<url>
```

- `<url>` URL and name of the file containing the emergency installation bundle image.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The boot flash is erased during the installation operation. After you perform the emergency install operation, set the BOOT variable in the ROMMON prompt by using the `set BOOT flash:packages.conf` command, and run the `boot flash:packages.conf` command manually in boot loader mode to boot the system. If the BOOT variable is not set in the ROMMON prompt, once the system has booted, set the BOOT variable in the device prompt by using the `boot system flash:packages.conf` command in global configuration mode.

**Usage Guidelines**

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:

Downloading bundle tftp:

Validating bundle tftp:

Installing bundle tftp:

Verifying bundle tftp:

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-iodsd-universalk9.SPA.150-1.0.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.

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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to exit the configuration mode:

```
Device(config)# exit
```

```
Device#
```
## factory-reset

To erase all customer-specific data and restore a device to its factory configuration, use the `factory-reset` command in privileged EXEC mode.

```
factory-reset {all | boot-vars | config}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>boot-vars</th>
<th>config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erases all the content from the NVRAM, all Cisco IOS images including the current boot image, boot variables, startup and running configuration data, and user data.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Erases only the user-added boot variables.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Erases only the startup configurations.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The `factory-reset` command is used in the following scenarios:

- To return a device to Cisco for Return Material Authorization (RMA), use this command to remove all the customer-specific data before obtaining an RMA certificate for the device.

- If the key information or credentials that are stored on a device is compromised, use this command to reset the device to factory configuration, and then reconfigure the device.

After the factory reset process is successfully completed, the device reboots and enters ROMmon mode.

### Examples

The following example shows how to erase all the content from a device using the `factory-reset all` command

```
Device> enable
Device# factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units (USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```
To initialize the flash: filesystem, use the `flash_init` command in boot loader mode.

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

### Command Default
The flash: filesystem is automatically initialized during normal system operation.

### Command Modes
Boot loader

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
During the normal boot process, the flash: filesystem is automatically initialized.

Use this command to manually initialize the flash: filesystem. 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
To install Software Maintenance Upgrade (SMU) packages, use the `install` command in privileged EXEC mode.

```
```

### Syntax Description

- **abort**
  Terminates the current install operation.

- **activate**
  Validates whether the SMU is added through the `install add` command.

  This keyword runs a compatibility check, updates package status, and if the package can be restarted, triggers post-install scripts to restart the necessary processes, or triggers a reload for nonrestartable packages.

- **file**
  Specifies the package to be activated.

- `{bootflash: | flash: | harddisk: | webui:}`
  Specifies the location of the installed package.

- **auto-abort-timer**
  (Optional) Installs an auto-abort timer.

- **prompt-level {all | none}**
  (Optional) Prompts a 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 prompts users about wanting to continue or not.

  The `all` keyword allows you to enable prompts. The `none` keyword disables prompts.

- **add**
  Copies files from a remote location (through FTP or TFTP) to a device and performs 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.


  Specifies the package to be added.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>commit</td>
<td>Makes SMU changes persistent over reloads. You can perform a commit after</td>
</tr>
<tr>
<td></td>
<td>activating a package while the system is up, or after the first reload. If</td>
</tr>
<tr>
<td></td>
<td>a package is activated, but not committed, it remains active after the first</td>
</tr>
<tr>
<td></td>
<td>reload, but not after the second reload.</td>
</tr>
<tr>
<td>auto-abort-timer stop</td>
<td>Stops the auto-abort timer.</td>
</tr>
<tr>
<td>deactivate</td>
<td>Deactivates an installed package.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Deactivating a package also updates the package status and might</td>
</tr>
<tr>
<td></td>
<td>trigger a process restart or reload.</td>
</tr>
<tr>
<td>label id</td>
<td>Specifies the ID of the install point to label.</td>
</tr>
<tr>
<td>description</td>
<td>Adds a description to the specified install point.</td>
</tr>
<tr>
<td>label-name name</td>
<td>Adds a label name to the specified install point.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes the installed packages. The <code>remove</code> keyword can only be used on</td>
</tr>
<tr>
<td></td>
<td>packages that are currently inactive.</td>
</tr>
<tr>
<td>inactive</td>
<td>Removes all the inactive packages from the device.</td>
</tr>
<tr>
<td>rollback</td>
<td>Rolls back the data model interface (DMI) package SMU to the base version,</td>
</tr>
<tr>
<td></td>
<td>the last committed version, or a known commit ID.</td>
</tr>
<tr>
<td>to base</td>
<td>Returns to the base image.</td>
</tr>
<tr>
<td>committed</td>
<td>Returns to the installation state when the last commit operation was</td>
</tr>
<tr>
<td></td>
<td>performed.</td>
</tr>
<tr>
<td>id install-ID</td>
<td>Returns to the specific install point ID. Valid values are from 1 to 4294967295.</td>
</tr>
</tbody>
</table>

**Command Default**

Packages are not installed.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>Hot-patching support is introduced. Sample output updated with hot SMU outputs.</td>
</tr>
</tbody>
</table>
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 contains a minimal set of files for patching the release along with metadata that describes the contents of the package.

Packages must be added before the SMU is activated.

A package must be deactivated before it is removed from Flash. A removed packaged must be added again.

The following example shows how to add an install package to a device:

```
Device# install add file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
install_add: START Mon Mar  5 21:48:51 PST 2018
install_add: Adding SMU
--- Starting initial file syncing ---
Info: Finished copying
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin to the selected switch(es)
Finished initial file syncing
Executing pre scripts....
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation
SUCCESS: install_add
```

The following example shows how to activate an install package:

```
Device# install activate file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin
install_activate: START Mon Mar  5 21:49:22 PST 2018
install_activate: Activating SMU
Executing pre scripts....
Executing pre scripts done.
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation
SUCCESS: install_activate
```

The following example shows how to commit an installed package:

```
```
Device# `install commit`

install_commit: START Mon Mar 5 21:50:52 PST 2018
install_commit: Committing SMU
Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit

/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon Mar 5 21:51:01 PST 2018

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show install</td>
<td>Displays information about the install packages.</td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>The command was introduced.</td>
</tr>
</tbody>
</table>

**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 boot level

To boot a new software license on the device, use the `license boot level` command in global configuration mode. Use the `no` form of this command to remove all software licenses from the device.

`license boot level base-license-level addon addon-license-level
no license boot level`

**Syntax Description**

- `base-license-level` Level at which the switch is booted, for example, `network-essentials`
  - Base licenses that are available are:
    - Network Essentials
    - Network Advantage (includes Network Essentials)

- `addon-license-level` Additional licenses that can be subscribed for a fixed term of three, five, or seven years.
  - Add-on licenses that are available are:
    - Digital Networking Architecture (DNA) Essentials
    - DNA Advantage (includes DNA Essentials)

**Command Default**

The switch boots the configured image.

**Command Modes**

Global configuration (config)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `license boot level` command for these purposes:

- Downgrade or upgrade licenses
- Enable or disable an evaluation or extension license
- Clear an upgrade license

This command forces the licensing infrastructure to boot the configured license level instead of the license hierarchy maintained by the licensing infrastructure for a given module:

- When the switch reloads, the licensing infrastructure checks the configuration in the startup configuration for licenses, if any. If there is a license in the configuration, the switch boots with that license. If there is no license, the licensing infrastructure follows the image hierarchy to check for licenses.
- If the forced boot evaluation license expires, the licensing infrastructure follows the regular hierarchy to check for licenses.
- If the configured boot license has already expired, the licensing infrastructure follows the hierarchy to check for licenses.
The following example shows how to activate the `network-essentials` license on a switch at the next reload:

```
Device(config)# license boot level network-essentials
```
**license smart deregister**

To cancel device registration from Cisco Smart Software Manager (CSSM), use the `license smart deregister` command in privileged EXEC mode.

```plaintext
license smart deregister
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use the `license smart deregister` command for these purposes:

- When your device is taken off the inventory
- When your device is shipped elsewhere for redeployment
- When your device is returned to Cisco for replacement using the return merchandise authorization (RMA) process

**Example**

This example shows how to deregister a device from CSSM:

```
Device# license smart deregister
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-AGENT_DEREG_SUCCESS: Smart Agent for Licensing De-registration with the Cisco Smart Software Manager or satellite was successful
*Jun 25 00:20:13.291 PDT: %SMART_LIC-5-EVAL_START: Entering evaluation period
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features is Not Allowed for udi PID:ISR4461/K9,SN:FDO2213A0GL
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>license smart register idtoken</td>
<td>Registers a device in CSSM.</td>
</tr>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
</tbody>
</table>
To register a device with the token generated from Cisco Smart Software Manager (CSSM), use the `license smart register idtoken` command in privileged EXEC mode.

```
license smart register idtoken token_ID {force}
```

**Syntax Description**

- **token_ID**: Device with the token generated from CSSM.
- **force**: Forcefully registers your device irrespective of whether the device is registered or not.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to register a device on CSSM:

```
Device# license smart register idtoken
$T14UytrNXzbEs1ck8veUtWaG5abnZJOFDd1FwbVRA%0Ab1RMbs0%3D%0A
Registration process is in progress. Use the 'show license status' command to check the progress and result
Device#% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 0 seconds)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>license smart deregister</code></td>
<td>Cancels the device registration from CSSM.</td>
</tr>
<tr>
<td><code>show license all</code></td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td><code>show license status</code></td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td><code>show license summary</code></td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td><code>show license usage</code></td>
<td>Displays license usage information</td>
</tr>
</tbody>
</table>
**license smart renew**

To manually renew your device's ID or authorization with Cisco Smart Software Manager (CSSM), use the `license smart renew` command in privileged EXEC mode.

```
license smart renew {auth | id}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>auth</th>
<th>Renews your authorization.</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Renews your ID.</td>
</tr>
</tbody>
</table>

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Authorization periods are renewed by the smart licensing system every 30 days. As long as the license is in an Authorized or Out of compliance state, the authorization period is renewed. The grace period starts when an authorization period expires. During the grace period or when the license is in the Expired state, the system continues to try and renew the authorization period. If a retry is successful, a new authorization period starts.

**Example**

This example shows how to renew a device license:

```
Device# license smart renew auth
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
</tbody>
</table>
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.

```plaintext
location {admin-tag string | civic-location identifier {host id} | civic-location identifier {host id} |
elin-location {string | identifier id} | geo-location identifier {host id} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location {admin-tag string | civic-location identifier {host id} | civic-location identifier {host id} |
elin-location {string | identifier id} | geo-location identifier {host id} | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

**Syntax Description**

- `admin-tag string`: 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.
- `id`: Name of the civic, emergency, or geographical location.

**Note**
The identifier for the civic location in the LLDP-MED switch TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.

- `elin-location`: Configures emergency location information (ELIN).
- `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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:

```bash
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:

```bash
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:

```bash
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

- **Release**
  - Cisco IOS XE Everest 16.5.1a
  - 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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>filesystem</code></td>
<td>Alias for a file system. Use <code>usbflash0:</code> for USB memory sticks.</td>
</tr>
<tr>
<td><code>/directory-url...</code></td>
<td>Name of the directories to create. Separate each directory name with a space.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

**Example**

This example shows how to make a directory called `Saved_Configs`:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```
**more**

To display the contents of one or more files, use the `more` command in boot loader mode.

```
more filesystem:/file-url...
```

**Syntax Description**

`filesystem:` Alias for a file system. Use `flash:` for the system board flash device.

`/file-url...` Path (directory) and name of the files to display. Separate each filename with a space.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Privileged EXEC</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command History</td>
</tr>
<tr>
<td>Release</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Cisco IOS XE Release 16.1</td>
</tr>
</tbody>
</table>

Example:

This example shows how to disable debugging on a switch.

```
Device: no debug all
All possible debugging has been turned off.
```
rename

To rename a file, use the rename command in boot loader mode.

rename filesystem:/source-file-url filesystem:/destination-file-url

**Syntax Description**

- **filesystem:** Alias for a file system. Use **usbflash0:** for USB memory sticks.
- **/source-file-url** Original path (directory) and filename.
- **/destination-file-url** New path (directory) and filename.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 consent-token accept-response shell-access

To submit the Consent Token response to a previously generated challenge, use the request consent-token accept-response shell-access command.

request consent-token accept-response shell-access response-string

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>response-string</td>
<td>Specifies the character string representing the response.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC mode (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

You must enter the response string within 30 minutes of challenge generation. If it is not entered, the challenge expires and a new challenge must be requested.

Example

The following is sample output from the request consent-token accept-response shell-access response-string command:

Device# request consent-token accept-response shell-access
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success: Shell access 0).
request consent-token generate-challenge shell-access

To generate a Consent Token challenge for system shell access, use the request consent-token generate-challenge shell-access command.

request consent-token generate-challenge shell-access auth-timeout time-validity-slot

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth-timeout time-validity-slot</td>
<td>Specifies the time slot in minutes for which shell-access is requested.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC mode (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

When the requested time-slot for system shell expires, the session gets terminated automatically. The maximum authorization timeout for system shell access is seven days.

Example

The following is sample output from the request consent-token generate-challenge shell-access auth-timeout time-validity-slot command:

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
zSSdrAAAAQEBAAQAAAABAgAEAAAAAAMACH86csUhmDl0BAAQ0Fvd7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEFfREVNTwcAGENUQV9ERU1PX0NUQV9TSUdOSU5HX0tFWQgAC0M5ODAwLUNMLUs5CQALOVpQUEVESE5KRkI=
Device#
```

*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation attempt: Shell access 0).
request consent-token terminate-auth

To terminate the Consent Token based authorization to system shell, use the `request consent-token terminate-auth` command.

**request consent-token terminate-auth**

**Command Modes**

<table>
<thead>
<tr>
<th>Command Modes</th>
<th>Privileged EXEC mode (#)</th>
</tr>
</thead>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.11.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

In system shell access scenario, exiting the shell does not terminate authorization until the authorization timeout occurs.

We recommend that you force terminate system shell authorization by explicitly issuing the `request consent-token terminate-auth` command once the purpose of system shell access is complete.

If the current authentication is terminated using the `request consent-token terminate-auth` command, the user will have to repeat the authentication process to gain access to system shell.

**Example**

The following is sample output from the `request consent-token terminate-auth` command:

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success

Device#
Device#
```


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 3650/3850/9200/9300 switches), this command can only be used to start a session on the standby console. On Catalyst 9500 switches, this command is supported only in a stackwise virtual setup. 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.
  
  **Note** This argument is not supported on Catalyst 9500 switches.
- **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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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#
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced</td>
<td>Supports advanced features such as NetFlow.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No default behavior or values.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Modes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Global configuration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td></td>
</tr>
<tr>
<td>Cisco IOS XE Everest</td>
<td></td>
</tr>
<tr>
<td>16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```
service private-config-encryption

To enable private configuration file encryption, use the `service private-config-encryption` command. To disable this feature, use the `no` form of this command.

```
service private-config-encryption
no service private-config-encryption
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default behavior or values.

### Command Modes

Global configuration (config)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.8.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable private configuration file encryption:

```
Device> enable
Device# configure terminal
Device(config)# service private-config-encryption
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show parser encrypt file status</code></td>
<td>Displays the private configuration encryption status.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>variable</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>MANUAL_BOOT</code></td>
<td>—Decides whether the device boots automatically or manually. 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.</td>
</tr>
<tr>
<td><code>BOOT filesystem:/file-url</code></td>
<td>—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting. If the <code>BOOT</code> 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 <code>BOOT</code> 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.</td>
</tr>
<tr>
<td><code>ENABLE_BREAK</code></td>
<td>—Allows the automatic boot process to be interrupted when the user presses the <code>Break</code> key on the console. Valid values are 1, Yes, On, 0, No, and Off. If set to 1, Yes, or On, you can interrupt the automatic boot process by pressing the <code>Break</code> key on the console after the flash: file system has initialized.</td>
</tr>
<tr>
<td><code>HELPER filesystem:/file-url</code></td>
<td>—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.</td>
</tr>
<tr>
<td><code>PS1 prompt</code></td>
<td>—Specifies a string that is used as the command-line prompt in boot loader mode.</td>
</tr>
<tr>
<td><code>CONFIG_FILE flash:/file-url</code></td>
<td>—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</td>
</tr>
<tr>
<td><code>BAUD rate</code></td>
<td>—Specifies the number of bits per second (b/s) that is used for the baud rate for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 128000 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000. The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</td>
</tr>
<tr>
<td><code>SWITCH_NUMBER stack-member-number</code></td>
<td>—Changes the member number of a stack member.</td>
</tr>
<tr>
<td><code>SWITCH_PRIORITY priority-number</code></td>
<td>—Changes the priority value of a stack member.</td>
</tr>
</tbody>
</table>

**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).

PSI 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 equals 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

---

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show avc client` command:

```
Device# sh avc client 0040.96ae.65ec top 10 application aggregate
```

**Cumulative Stats:**

<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>skinny</td>
<td>7343</td>
<td>449860</td>
<td>61</td>
<td>94</td>
</tr>
<tr>
<td>2</td>
<td>unknown</td>
<td>99</td>
<td>13631</td>
<td>137</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>dhcp</td>
<td>18</td>
<td>8752</td>
<td>486</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>http</td>
<td>18</td>
<td>3264</td>
<td>181</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>tftp</td>
<td>9</td>
<td>534</td>
<td>59</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>dns</td>
<td>2</td>
<td>224</td>
<td>112</td>
<td>0</td>
</tr>
</tbody>
</table>

**Last Interval (90 seconds) Stats:**

<table>
<thead>
<tr>
<th>No.</th>
<th>AppName</th>
<th>Packet-Count</th>
<th>Byte-Count</th>
<th>AvgPkt-Size</th>
<th>usage%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>skinny</td>
<td>9</td>
<td>540</td>
<td>60</td>
<td>100</td>
</tr>
</tbody>
</table>
show debug

To display all the debug commands available on a switch, use the `show debug` command in Privileged EXEC mode.

```
show debug

show debug condition Condition identifier | All conditions
```

**Syntax Description**
- **Condition identifier**: Sets the value of the condition identifier to be used. Range is between 1 and 1000.
- **All conditions**: Shows all conditional debugging options available.

**Command Default**
No default behavior or values.

**Command Modes**
Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Release 16.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays fan, temperature and power environmental status.</td>
</tr>
<tr>
<td>fan</td>
<td>Displays the switch fan status.</td>
</tr>
<tr>
<td>power</td>
<td>Displays the power supply status.</td>
</tr>
<tr>
<td>all</td>
<td>(Optional) Displays the status for all power supplies.</td>
</tr>
<tr>
<td>switch switch-number</td>
<td>(Optional) Displays the power supply status for a specific switch.</td>
</tr>
<tr>
<td>stack stack-number</td>
<td>(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.</td>
</tr>
<tr>
<td>temperature</td>
<td>Displays the switch temperature status.</td>
</tr>
<tr>
<td>status</td>
<td>(Optional) Displays the temperature status and threshold values.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

User EXEC

Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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 165: States in the show env temperature status Command Output

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
<td>The switch temperature is in the <em>normal</em> operating range.</td>
</tr>
<tr>
<td>Yellow</td>
<td>The temperature is in the <em>warning</em> range. You should check the external temperature around the switch.</td>
</tr>
<tr>
<td>Red</td>
<td>The temperature is in the <em>critical</em> range. The switch might not run properly if the temperature is in this range.</td>
</tr>
</tbody>
</table>
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 }
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>budgeting</td>
<td>Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the <code>show env xps configuration</code> command to retrieve the non-default configuration.</td>
</tr>
<tr>
<td>port [ all</td>
<td>number ]</td>
</tr>
<tr>
<td>power</td>
<td>Displays the status of the XPS power supplies.</td>
</tr>
<tr>
<td>system</td>
<td>Displays the XPS system status.</td>
</tr>
<tr>
<td>thermal</td>
<td>Displays the XPS thermal status.</td>
</tr>
<tr>
<td>upgrade</td>
<td>Displays the XPS upgrade status.</td>
</tr>
<tr>
<td>version</td>
<td>Displays the XPS version details.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.2(55)SE1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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# show env xps budgeting
---
XPS 0101.0100.0000 :
---------------------------------------------------------
<table>
<thead>
<tr>
<th>Data</th>
<th>Current</th>
<th>Power</th>
<th>Power Port</th>
<th>Switch #</th>
<th>PS A</th>
<th>PS B</th>
<th>Role-State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committed Budget</td>
<td>----</td>
<td>----</td>
<td>---------</td>
<td>--------</td>
<td>----</td>
<td>----</td>
<td>----------</td>
</tr>
<tr>
<td>223</td>
<td>1543</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

---

**Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)**
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
```
This is an example of output from the show env xps system command:

Switch#

---

XPS 0101.0100.0000:

<table>
<thead>
<tr>
<th>XPS</th>
<th>Cfg</th>
<th>Cfg</th>
<th>RPS Switch</th>
<th>Current</th>
<th>Data Port</th>
<th>XPS Port Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Role</td>
<td>Pri Conn</td>
<td>Role-State</td>
<td>Switch #</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----</td>
<td>----</td>
<td>-------</td>
<td>----------</td>
<td>--------</td>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>On Auto-SP</td>
<td>1 Yes</td>
<td>SP-PS</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>On Auto-SP</td>
<td>2 Yes</td>
<td>SP-PS</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>-</td>
<td>On Auto-SP</td>
<td>3 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>none</td>
<td>On Auto-SP</td>
<td>5 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>-</td>
<td>Off Auto-SP</td>
<td>6 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>On Auto-SP</td>
<td>7 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>-</td>
<td>On Auto-SP</td>
<td>8 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>On Auto-SP</td>
<td>9 No</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>test</td>
<td>On Auto-SP</td>
<td>4 Yes</td>
<td>RPS-NB</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This is an example of output from the show env xps thermal command:

Switch#

---

Fan Status

<table>
<thead>
<tr>
<th>Fan Status</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 OK</td>
<td></td>
</tr>
<tr>
<td>2 OK</td>
<td></td>
</tr>
<tr>
<td>3 NOT PRESENT PS-1</td>
<td></td>
</tr>
<tr>
<td>NOT PRESENT PS-2</td>
<td></td>
</tr>
<tr>
<td>OK Temperature is OK</td>
<td></td>
</tr>
</tbody>
</table>

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

SW Status Prog

*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

SW Status Prog

*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has started through the Service Port.*
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 166: Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>power xps (global configuration command)</td>
<td>Configures XPS and XPS port names.</td>
</tr>
<tr>
<td>power xps (privileged EXEC command)</td>
<td>Configures the XPS ports and system.</td>
</tr>
</tbody>
</table>
show flow monitor

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

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>(Optional) Specifies the name of a flow monitor.</td>
</tr>
<tr>
<td><strong>monitor-name</strong></td>
<td>(Optional) Name of a flow monitor that was previously configured.</td>
</tr>
<tr>
<td><strong>cache</strong></td>
<td>(Optional) Displays the contents of the cache for the flow monitor.</td>
</tr>
<tr>
<td><strong>format</strong></td>
<td>(Optional) Specifies the use of one of the format options for formatting the display output.</td>
</tr>
<tr>
<td><strong>csv</strong></td>
<td>(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.</td>
</tr>
<tr>
<td><strong>record</strong></td>
<td>(Optional) Displays the flow monitor cache contents in record format.</td>
</tr>
<tr>
<td><strong>table</strong></td>
<td>(Optional) Displays the flow monitor cache contents in table format.</td>
</tr>
<tr>
<td><strong>statistics</strong></td>
<td>(Optional) Displays the statistics for the flow monitor.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

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

The uppercase field names in the display output of the **show flow monitor monitor-name cache** command are key fields that use 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 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
```

This table describes the significant fields shown in the display.
Table 167: show flow monitor monitor-name Field Descriptions

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

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

This table describes the significant fields shown in the display.

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

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:

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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Name: cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version: 16.6.1.0.199.1484082952..Everest
Platform: Catalyst3k
Package Type: dmp
Defect ID: CSCxxx
Package State: Added
Supersedes List: {}
Smu ID: 1
```
The following is sample output from the `show install summary` command:

```
Device# show install summary

Active Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
  No packages
Committed Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
  No packages
Device#
```

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

**Table 168: show install summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Packages</td>
<td>Name of the active install package.</td>
</tr>
<tr>
<td>Inactive Packages</td>
<td>List of inactive packages.</td>
</tr>
<tr>
<td>Committed Packages</td>
<td>Install packages that have saved or committed changes to the harddisk, so that the changes become persistent across reloads.</td>
</tr>
<tr>
<td>Uncommitted Packages</td>
<td>Install package activations that are nonpersistent.</td>
</tr>
</tbody>
</table>

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/cat3k-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>install</td>
<td>Installs SMU packages.</td>
</tr>
</tbody>
</table>
show license all

To display the entitlement information, use the `show license all` command in privileged EXEC mode.

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

### Command Default
Privileged EXEC (#)

### Command History
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines
The command also displays whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on.

### Example
This example shows a sample output from the `show license all` command:

```
Device# show license all
Smart Licensing Status
----------------------
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 16 09:44:50 2018 IST
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 12 09:44:49 2019 IST
  Registration Expires: Jul 16 09:39:05 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 31 17:30:02 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 31 17:30:02 2018 IST
  Next Communication Attempt: Aug 30 17:30:01 2018 IST
  Communication Deadline: Oct 29 17:24:12 2018 IST

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
```
Type: Callhome

License Usage
===============

C9500 48Y4C DNA Advantage (C9500-DNA-48Y4C-A):
  Description: C9500 48Y4C DNA Advantage
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

C9500 48Y4C NW Advantage (C9500-48Y4C-A):
  Description: C9500 48Y4C NW Advantage
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
  Export status: NOT RESTRICTED

Product Information
====================
UDI: PID:C9500-48Y4C,SN:CAT2150L5HK

Agent Version
==============
Smart Agent for Licensing: 4.5.2_rel/32
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
================
License reservation: DISABLED

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td>show license udi</td>
<td>Displays UDI.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
<tr>
<td>show tech-support license</td>
<td>Displays the debug output.</td>
</tr>
</tbody>
</table>
**show license status**

To display the compliance status of a license, use the `show license status` command in privileged EXEC mode.

**show license status**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output from the `show license status` command:

```
Device# show license status
Smart Licensing is ENABLED

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED
Smart Account: Cisco Systems
Virtual Account: NPR
Export-Controlled Functionality: Allowed
Initial Registration: First Attempt Pending
Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
Next Renewal Attempt: Jan 15 14:49:47 2019 IST
Registration Expires: Jul 19 14:43:47 2019 IST

License Authorization:
Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
Next Communication Attempt: Aug 27 07:02:56 2018 IST
Communication Deadline: Oct 26 06:57:50 2018 IST
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td>show license udi</td>
<td>Displays UDI.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
<tr>
<td>show tech-support license</td>
<td>Displays the debug output.</td>
</tr>
</tbody>
</table>
show license summary

To display a summary of all active licenses, use the **show license summary** command in privileged EXEC mode.

### show license summary

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows a sample output from the **show license summary** command:

```
Device# show license summary  Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 12 09:44:49 2019 IST

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 30 17:30:02 2018 IST

License Usage:

<table>
<thead>
<tr>
<th>License</th>
<th>Entitlement tag</th>
<th>Count Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500 48Y4C DNA Advan...</td>
<td>(C9500-DNA-48Y4C-A)</td>
<td>1 AUTHORIZED</td>
</tr>
<tr>
<td>C9500 48Y4C NW Advan...</td>
<td>(C9500-48Y4C-A)</td>
<td>1 AUTHORIZED</td>
</tr>
</tbody>
</table>
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>show license udi</td>
<td>Displays UDI.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
<tr>
<td>show tech-support license</td>
<td>Displays the debug output.</td>
</tr>
</tbody>
</table>
show license udi

To display the Unique Device Identifier (UDI), use the show license udi command in privileged EXEC mode.

**show license udi**

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output from the show license udi command:

```
Device# show license udi
UDI: PID:C9500-48Y4C,SN:CAT2150L5HK
```
show license usage

To display license usage information, use the show license usage command in privileged EXEC mode.

show license usage

This command has no arguments or keywords.

Command Default

<table>
<thead>
<tr>
<th>Command Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Example

This example shows a sample output from the show license usage command:

Device# show license usage
License Authorization:
    Status: AUTHORIZED on Jul 31 17:30:02 2018 IST

C9500 48Y4C DNA Advantage (C9500-DNA-48Y4C-A):
    Description: C9500 48Y4C DNA Advantage
    Count: 1
    Version: 1.0
    Status: AUTHORIZED
    Export status: NOT RESTRICTED

C9500 48Y4C NW Advantage (C9500-48Y4C-A):
    Description: C9500 48Y4C NW Advantage
    Count: 1
    Version: 1.0
    Status: AUTHORIZED
    Export status: NOT RESTRICTED

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td>show license udi</td>
<td>Displays UDI.</td>
</tr>
<tr>
<td>show tech-support license</td>
<td>Displays the debug output.</td>
</tr>
</tbody>
</table>
# show location

To display location information for an endpoint, use the `show location` command in privileged EXEC mode.

```
show location
[

    admin-tag
    civic-location
    custom-location
    elin-location
    geo-location

    identifier identifier-string
    interface type number
    static

    admin-tag
    civic-location
    custom-location
    elin-location
    geo-location

    identifier identifier-string
    interface type number
    static

    admin-tag
    civic-location
    custom-location
    elin-location
    geo-location

    identifier identifier-string
    interface type number
    static

    admin-tag
    civic-location
    custom-location
    elin-location
    geo-location

    identifier identifier-string
    interface type number
    static

show location
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin-tag</td>
<td>Displays administrative tag or site information.</td>
</tr>
<tr>
<td>civic-location</td>
<td>Specifies civic location information.</td>
</tr>
<tr>
<td>identifier</td>
<td>Information identifier of the civic location, custom location, or geo-spatial location.</td>
</tr>
<tr>
<td>interface type number</td>
<td>For information about the numbering syntax for your device, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>static</td>
<td>Displays configured civic, custom, or geo-spatial location information.</td>
</tr>
<tr>
<td>custom-location</td>
<td>Specifies custom location information.</td>
</tr>
<tr>
<td>elin-location</td>
<td>Specifies emergency location information (ELIN).</td>
</tr>
<tr>
<td>geo-location</td>
<td>Specifies geo-spatial location information.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the civic, custom, or geo-spatial host location information.</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The following sample output of the `show location civic-location` command displays civic location information for the specified identifier (identifier 1):

```
Device# show location civic-location identifier 1
Civic location information
-----------------------------
Identifier : 1
County : Santa Clara
Street number : 3550
Building : 19
Room : C6
Primary road name : Example
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Configures location information for an endpoint.</td>
</tr>
</tbody>
</table>

City: San Jose  
State: CA  
Country: US
show logging onboard switch uptime

To display a history of all reset reasons for all modules or switches in a system, use the `show logging onboard switch uptime` command.

```
show logging onboard switch { switch-number | active | standby } uptime [ [ continuous | detail ] [ start hour day month [ year ] [ end hour day month year ] ] ] | summary
```

**Syntax Description**

- **switch switch-number** Specifies a switch. Enter the switch number.
- **active** Specifies the active instance.
- **standby** Specifies the standby instance.
- **continuous** (Optional) Displays continuous data.
- **detail** (Optional) Displays detailed data.
- **start hour day month year** (Optional) Specifies the start time to display data.
- **end hour day month year** (Optional) Specifies the end time to display data.
- **summary** (Optional) Displays summary data.

**Command Modes**

Privileged EXEC(#)  

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was implemented on the Cisco Catalyst 9500 Series Switches</td>
</tr>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>The output of this command was updated to display the reload reasons for members in a stack.</td>
</tr>
</tbody>
</table>

**Examples:**

The following is a sample output from the `show logging onboard switch active uptime continuous` command:

```
Device# show logging onboard switch active uptime continuous
--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp | Reset | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours minutes
--------------------------------------------------------------------------------
06/17/2018 19:42:56 | Reload | 0 0 0 0 5
06/17/2018 19:56:31 | Reload | 0 0 0 0 5
06/17/2018 20:10:46 | Reload | 0 0 0 0 5
06/17/2018 20:23:48 | Reload | 0 0 0 0 5
06/17/2018 20:37:20 | Reload Command | 0 0 0 0 5
06/18/2018 17:09:23 | Reload Command | 0 0 0 20 5
06/18/2018 17:18:39 | redundancy force-switchover | 0 0 0 0 5
06/18/2018 18:33:33 | Reload | 0 0 0 1 5
06/18/2018 19:03:05 | Reload | 0 0 0 0 5
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following is a sample output from the `show logging onboard switch active uptime detail` command:

```
Device# show logging onboard switch active uptime detail

UPTIME SUMMARY INFORMATION
First customer power on: 06/10/2017 09:28:22
Total uptime: 0 years 50 weeks 4 days 13 hours 38 minutes
Total downtime: 0 years 15 weeks 4 days 11 hours 52 minutes
Number of resets: 75
Number of slot changes: 9
Current reset reason: PowerOn
Current slot: 1
Chassis type: 0
Current uptime: 0 years 0 weeks 0 days 0 hours 0 minutes

UPTIME CONTINUOUS INFORMATION

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Reset</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM/DD/YYYY HH:MM:SS</td>
<td>Reason</td>
<td>years weeks days hours minutes</td>
</tr>
<tr>
<td>06/10/2017 09:28:22</td>
<td>Reload</td>
<td>0 0 0 0 5</td>
</tr>
<tr>
<td>09/17/2018 09:07:44</td>
<td>PowerOn</td>
<td>0 0 3 15 5</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show logging onboard switch standby uptime detail` command:

```
Device# show logging onboard switch standby uptime detail

UPTIME SUMMARY INFORMATION

UPTIME CONTINUOUS INFORMATION

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Reset</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM/DD/YYYY HH:MM:SS</td>
<td>Reason</td>
<td>years weeks days hours minutes</td>
</tr>
<tr>
<td>09/17/2018 10:16:26</td>
<td>Reload Command</td>
<td>0 0 0 1 5</td>
</tr>
<tr>
<td>09/17/2018 10:59:57</td>
<td>PowerOn</td>
<td>0 0 0 0 5</td>
</tr>
</tbody>
</table>
```
First customer power on: 06/10/2017 11:51:26
Total uptime: 0 years 46 weeks 0 days 11 hours 44 minutes
Total downtime: 0 years 20 weeks 1 days 10 hours 45 minutes
Number of resets: 79
Number of slot changes: 13
Current reset reason: PowerOn
Current slot: 2
Chassis type: 0
Current uptime: 0 years 0 weeks 0 days 0 hours 5 minutes

<table>
<thead>
<tr>
<th>Time Stamp</th>
<th>Reset</th>
<th>Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM/DD/YYYY HH:MM:SS</td>
<td>Reason</td>
<td>years weeks days hours minutes</td>
</tr>
<tr>
<td>06/10/2017 11:51:26</td>
<td>Reload</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>&lt;snip&gt;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08/10/2018 09:13:58</td>
<td>LocalSoft</td>
<td>0 0 2 5 4</td>
</tr>
<tr>
<td>08/28/2018 14:21:42</td>
<td>Reload Slot Command</td>
<td>0 0 0 3 5</td>
</tr>
<tr>
<td>08/28/2018 14:34:29</td>
<td>System requested reload</td>
<td>0 0 0 0 0</td>
</tr>
<tr>
<td>09/11/2018 09:08:15</td>
<td>Reload</td>
<td>0 0 1 8 5</td>
</tr>
<tr>
<td>09/11/2018 19:15:06</td>
<td>redundancy force-switchover</td>
<td>0 0 0 9 4</td>
</tr>
<tr>
<td>09/13/2018 16:50:18</td>
<td>Reload Command</td>
<td>0 0 1 21 6</td>
</tr>
<tr>
<td>09/17/2018 10:55:09</td>
<td>PowerOn</td>
<td>0 0 0 0 5</td>
</tr>
</tbody>
</table>

The following is a sample output from the `show logging onboard switch active uptime summary` command:

```
Device# show logging onboard switch active uptime summary

UPTIME SUMMARY INFORMATION
First customer power on: 04/26/2018 21:45:39
Total uptime: 0 years 20 weeks 2 days 12 hours 22 minutes
Total downtime: 0 years 2 weeks 2 days 8 hours 40 minutes
Number of resets: 1900
Number of slot changes: 18
Current reset reason: Reload Command
Current reset timestamp: 09/26/2018 20:43:15
Current slot: 1
Chassis type: 91
Current uptime: 0 years 0 weeks 5 days 22 hours 5 minutes
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
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.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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 pkp buf unavail cnt : 0
Xmt last interface : None
```
show parser encrypt file status

To view the private configuration encryption status, use the `show parser encrypt file status` command.

**show parser encrypt file status**

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

**Command Default**
None

**Command Modes**
User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.8.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following command output indicates that the feature is available and the file is encrypted. The file is in ‘cipher text’ format.

```
Device> enable
Device# show parser encrypt file status
Feature: Enabled
File Format: Cipher text
Encryption Version: ver1
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>service private-config-encryption</code></td>
<td>Enables private configuration file encryption.</td>
</tr>
</tbody>
</table>
show platform hardware fpga

To display the system field-programmable gate array (FPGA) settings, use the `show platform hardware fpga` command in privileged EXEC mode.

**show platform hardware fpga**

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

**Command Default**
None

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

The following is a sample output from the `show platform hardware fpga` command on a Cisco Catalyst 9300 Series switch:

```
Device# show platform hardware fpga

Register Addr  | FPGA Reg Description     | Value  
-----------------|--------------------------|--------
0x00000000      | Board ID                 | 0x00006053
0x00000004      | FPGA Version             | 0x00000206
0x00000008      | Reset Reg1               | 0x00010204
0x0000000c      | Reset Reg2               | 0x00000000
0x00000028      | FRU LED DATA Reg1        | 0x00001004
0x0000002c      | FRU LED DATA Reg2        | 0x00000000
0x00000030      | FRU Control Reg          | 0x00002020
0x00000034      | Doppler Misc Reg         | 0x00000000
0x00000038      | SBC Enable               | 0x00000000

<snip>
```

The following is a sample output from the `show platform hardware fpga` command on a Cisco Catalyst 9500 Series switch:

```
Device# show platform hardware fpga

Register Addr  | FPGA Reg Description     | Value  
-----------------|--------------------------|--------
0x00000000      | FPGA Version             | 0x00000110
0x00000004      | FRU Power Ctrl Reg       | 0x00000112
0x00000020      | System Reset Ctrl Reg    | 0x00000000
0x00000024      | Beacon LED Ctrl Reg      | 0x00000000
0x00000044      | 1588 Sync Pulse Reg      | 0x00000000
0x00000068      | Mainboard Misc Ctrl Reg  | 0x00000000
0x00000078      | DopplerD Misc Ctrl Reg   | 0x00000000

<snip>
```
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

- **Modification**: This command was introduced.

Examples

This example shows how to view the checksum record for boot stages:

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D98BDDE3E468DD27EB93F4A606006A0B70062928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA26684832924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature: 816C5A29741BBAC1961C109FFC36DA5459A4DBF211025F539AFB4868EF91834C05789
5DAFBC77474F301916B7D0D08ABE5E05E66598426A33E922021C2504383228B6787B74
8526A305B17DDA3CF8705BACFD5A2D55A333415CABC73DAFDEEFDF8777A77F482EC4B
731A0926A41FB3EFFC46DC02FBA666534DBEC7DCC0C02929DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE564E304
EE1D2A9C53E93E05B24A923BE8261199CED8DBA0CE7134596FF8D2D6E6DA773757C70C
D3BA31C45A91268C246DF32658999276F972153ABE823F0ACFE93BF0AD1A00E257
4E4CC41C945015A59FB8FE
Platform: WS-C3650-12X48UZ
```
show platform software audit

To display the SE Linux Audit logs, use the `show platform software audit` command in privileged EXEC mode.

```
show platform software audit { all | summary | [switch { switch-number | active | standby } ]
{ 0 | F0 | R0 | { FP | RP } { active } }}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Shows the audit log from all the slots.</td>
</tr>
<tr>
<td>summary</td>
<td>Shows the audit log summary count from all the slots.</td>
</tr>
<tr>
<td>switch</td>
<td>Shows the audit logs for a slot on a specific switch.</td>
</tr>
<tr>
<td>switch-number</td>
<td>Selects the switch with the specified switch number.</td>
</tr>
<tr>
<td>switch active</td>
<td>Selects the active instance of the switch.</td>
</tr>
<tr>
<td>standby</td>
<td>Selects the standby instance of the switch.</td>
</tr>
<tr>
<td>0</td>
<td>Shows the audit log for the SPA-Inter-Processor slot 0.</td>
</tr>
<tr>
<td>F0</td>
<td>Shows the audit log for the Embedded-Service-Processor slot 0.</td>
</tr>
<tr>
<td>R0</td>
<td>Shows the audit log for the Route-Processor slot 0.</td>
</tr>
<tr>
<td>FP active</td>
<td>Shows the audit log for the active Embedded-Service-Processor slot.</td>
</tr>
<tr>
<td>RP active</td>
<td>Shows the audit log for the active Route-Processor slot.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command was introduced in the Cisco IOS XE Gibraltar 16.10.1 as a part of the SELinux Permissive Mode feature. The `show platform software audit` command displays the system logs containing the access violation events.

In Cisco IOS XE Gibraltar 16.10.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the `show software platform software audit summary` command:
The following is a sample output of the `show software platform software audit all` command:

```
Device# show platform software audit all

AUDIT LOG ON switch 1
-----------------------------------
= START =

| type=AVC | msg=audit(153922292.584:100) | denied { read } for pid=14017 | comm="mcp_trace_filter" name="crashinfo" dev="rootfs" ino=13667 |
| tcontext=system_u:system_r:polaris_trace_filter_t:s0 |
| tcontext=system_u:object_r:polaris_disk_crashtest_t:s0 tclass=lnk_file permissive=1 |
| type=AVC msg=audit(153922292.584:100) | denied { getattr } for pid=14017 | comm="mcp_trace_filter" name="crashinfo" dev="rootfs" ino=13667 |
| tcontext=system_u:system_r:polaris_trace_filter_t:s0 |
| tcontext=system_u:object_r:polaris_disk_crashtest_t:s0 tclass=lnk_file permissive=1 |
| type=AVC msg=audit(1539438600.896:119) | denied { execute } for pid=8300 | comm="sh" name="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407 |
| tcontext=system_u:system_r:polaris_trace_filter_t:s0 |
| tcontext=system_u:object_r:polaris_auto_upgrade_server_rp_t:s0 tclass=dir permissive=1 |
| type=AVC msg=audit(1539438624.916:122) | denied { execute_no_trans } for pid=8600 | comm="auto_upgrade_shell" path="/bin/bash" dev="rootfs" ino=7276 |
| tcontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0 |
| tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1 |
| type=AVC msg=audit(1539438678.008:127) | denied { execute_no_trans } for pid=11579 | comm="auto_upgrade_shell" path="/bin/bash" dev="rootfs" ino=7276 |
| tcontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0 |
| tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1 |
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
The following is a sample output of the `show platform software audit switch` command:

```
Device# show platform software audit switch active R0

--- START ---

Device# show platform software audit switch active R0

--- END ---

```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)

System Management

show platform software audit
**show platform software fed switch punt cause**

To display information about why the packets received on an interface are puncted to the Router Processor (RP), use the `show platform software fed switch punt cpuq cause` command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} punt {cause_id | clear | summary}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`switch {switch-number</td>
<td>active</td>
</tr>
<tr>
<td></td>
<td>• <code>switch-number</code>.</td>
</tr>
<tr>
<td></td>
<td>• <code>active</code>—Displays information relating to the active switch.</td>
</tr>
<tr>
<td></td>
<td>• <code>standby</code>—Displays information relating to the standby switch, if available.</td>
</tr>
<tr>
<td><code>cause_id</code></td>
<td>Specifies the ID of the cause for which the details have to be displayed.</td>
</tr>
<tr>
<td><code>clear</code></td>
<td>Clears the statistics for all the causes. Clearing the causes might result in inconsistent statistics.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Displays a high-level overview of the punt reason.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

None

**Example**

The following is sample output from the `show platform software fed switch active punt cause summary` command.

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes

<table>
<thead>
<tr>
<th>Cause</th>
<th>Cause Info</th>
<th>Rcvd</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ARP request or response</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>RP&lt;-&gt;QFP keepalive</td>
<td>22314</td>
<td>0</td>
</tr>
<tr>
<td>55</td>
<td>For-us control</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td>60</td>
<td>IP subnet or broadcast packet</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>96</td>
<td>Layer2 control protocols</td>
<td>133808</td>
<td>0</td>
</tr>
</tbody>
</table>
```
The following is sample output from the `show platform software fed switch active punt cause cause-id` command.

Device# `show platform software fed switch active punt cause 21`  

**Detailed Statistics**

<table>
<thead>
<tr>
<th>Sub Cause</th>
<th>Rcvd</th>
<th>Dropped</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>22363</td>
<td>0</td>
</tr>
</tbody>
</table>

--------------------------------------------
show platform software fed switch punt cpuq

To display information about the punt traffic on CPU queues, use the show platform software fed switch punt cpuq command in privileged EXEC mode.

```
show platform software fed switch {switch-number | active | standby} punt cpuq {cpuq_id | all | brief | clear | rates}
```

### Syntax Description

- **switch** `{switch-number active standby}`
  - Displays information about the switch. You have the following options:
    - *switch-number*.
    - *active* — Displays information relating to the active switch.
    - *standby* — Displays information relating to the standby switch, if available.
  - **Note** This keyword is not supported.

- **punt**
  - Displays the punt information.

- **cpuq**
  - Displays information about the CPU receive queue.

- **cpuq_id**
  - Specifies details specific to a particular CPU queue.

- **all**
  - Displays the statistics for all the CPU queues.

- **brief**
  - Displays summarized statistics for all the queues like details about punt packets received and dropped.

- **clear**
  - Clears the statistics for all the CPU queues. Clearing the CPU queue might result in inconsistent statistics.

- **rates**
  - Displays the rate at which the packets are punted.

### Command Default

None

### Command Modes

Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

None
Example

The following is sample output from the `show platform software fed switch active punt cpuq brief` command.

```
Device# show platform software fed switch active punt cpuq brief
Punt CPU Q Statistics Brief
```

```
<table>
<thead>
<tr>
<th>Q no</th>
<th>Queue Name</th>
<th>Rx</th>
<th>Rx</th>
<th>Rx</th>
<th>Drop</th>
<th>Drop</th>
<th>Drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CPU_Q_DOT1X_AUTH</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>CPU_Q_L2_CONTROL</td>
<td>0</td>
<td>6772</td>
<td>6772</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>CPU_Q_FORUS_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>CPU_Q_ICMP_GEN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>CPU_Q_ROUTING_CONTROL</td>
<td>0</td>
<td>12</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>CPU_Q_FORUS_ADDR_RESOLUTION</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>CPU_Q_ICMP_REDIRECT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>CPU_Q_INTER_FED_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>CPU_Q_L2LVX_CONTROL_PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>CPU_Q_EWLC_CONTROL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>CPU_Q_EWLC_DATA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>11</td>
<td>CPU_Q_L2LVX_DATA_PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>CPU_Q_BROADCAST</td>
<td>0</td>
<td>21</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>CPU_Q_LEARNING_CACHE_OVFL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>CPU_Q_SW_FORWARDING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>CPU_Q_TOPOLOGY_CONTROL</td>
<td>0</td>
<td>127300</td>
<td>127300</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>16</td>
<td>CPU_Q_PROTO_SNOOPING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>CPU_Q_RBF_LOW_LATENCY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>18</td>
<td>CPU_Q_TRANSIT_TRAFFIC</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>19</td>
<td>CPU_Q_RPF_FAILED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>20</td>
<td>CPU_Q_MCAST_END_STATION_SERVICE</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>21</td>
<td>CPU_Q_LOGGING</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>22</td>
<td>CPU_Q_PUNT_WEBAUTH</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>23</td>
<td>CPU_Q_HIGH_RATE_APP</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>24</td>
<td>CPU_Q_EXCEPTION</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>25</td>
<td>CPU_Q_SYSTEM_CRITICAL</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>26</td>
<td>CPU_Q_NFL_SAMPLED_DATA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>27</td>
<td>CPU_Q_LOW_LATENCY</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>28</td>
<td>CPU_Q_EGR_EXCEPTION</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>29</td>
<td>CPU_Q_FSS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>30</td>
<td>CPU_Q_MCAST_DATA</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>31</td>
<td>CPU_Q_GOLD_PKT</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q no</td>
<td>ID of the queue.</td>
</tr>
<tr>
<td>Queue Name</td>
<td>Name of the queue.</td>
</tr>
<tr>
<td>Rx</td>
<td>Number of packets received.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop</td>
<td>Number of packets dropped.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show platform software fed switch active punt cpuq cpuq_id` command.

Device#```show platform software fed switch active punt cpuq 1```

Punt CPU Q Statistics
```
CPU Q Id : 1
CPU Q Name : CPU_Q_L2_CONTROL
Packets received from ASIC : 6774
Send to IOSd total attempts : 6774
Send to IOSd failed count : 0
RX suspend count : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count : 0
RX dropped count : 0
RX non-active dropped count : 0
RX conversion failure dropped : 0
RX INTACK count : 6761
RX packets dq'd after intack : 0
Active RxQ event : 6761
RX spurious interrupt : 0

Replenish Stats for all rxq:
```
Number of replenish : 61969
Number of replenish suspend : 0
Number of replenish un-suspend : 0
```
```
show platform sudi certificate

To display checksum record for the specific SUDI, use the `show platform sudi certificate` command in privileged EXEC mode.

```
Device# show platform sudi certificate
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoXwlA/Mnt/zANBgkqhkiG9w0BAQUFADAL
MRYwFAYDVQQKEw1DaXNjaByTeXN0Z1mZMrwGQYDVQQDEwJDaXNjaByBsb290IENB
ID1WNgDwHcNMDN0QWTE0MjAxNzEyEYWhcMjkwTE0MjA1MRYwFAYDVQQK
Ew1DaXNjaByBTeXN0Z1mZMrwGQYDVQQDEwJDaXNjaByBsb290IENBID1WNgDwHgEg
MA0GCGSGS1b3DQEBAQUAA4IBDAwggEiAMIBAgYIKwYBBQUHAwIwADAOBgNVHQ8BAQ
MR0gMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZ9Pdd+9aE2JbFkNjht6gfHKd477AkS5XAtUsSxokDYt/zBshl2Q3+3LR6qrgKQKvU6YJyH05YLBQcJ38s6NLk53905Wzp
9pRcmMCPu4x6cF/qR/u0iJ44medeDY2o3qPCpxzprJWbplc1MIYHUMQQmgm+g
xhFhIoW580BofcdnJyeBe5r27RuewW3mIpJ3Wd6bNQz6pFfjg66F+PSaweDkGB
BxG6j130veF+ryFWLfeF9j9f1/2+8oauY43QrvXN3d3/G6qFjXewv/szeX1kEd05FJXJ
UTvuMEJaJ53rd99jJwnkKHEpaeapsztr+kkvQ1DAQAb04BMCCAYwCwDVR8PBAdQD
ApHCM0B2G11dQzDB wk6vDNV7t8csmTr734MAP4fzaFbgNVHMSCEDA+WgQn
88qV6h6aAgkMrwWukIgfW2ranaDBgNVHR8EDEADM6igNqaAhQJNojikhWol8v3d3
LmNpc2NVlmNvbS9zZWN1cm10e59a2kv/Y3J2L2Ny2EyMDQ4LmNybDBQBqgrBqEF
-----END CERTIFICATE-----
```

```
Device# show platform sudi certificate
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgI4V88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3LmNpc2NvX1NQ
-----END CERTIFICATE-----
```
show romvar

To view all ROMMON environment variables, use the `show romvar` command. To view environmental variable for a specific resource, use the `show romvar | i resource_name`.

**show romvar**

<table>
<thead>
<tr>
<th>Command Default</th>
<th>This command has no arguments or keywords.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>Privileged EXEC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows the output from the `show romvar` command:

```
Device# show romvar
ROMMON variables:
BOARDID="20610"
MODEL_NUM="C9500-40X"
SYSTEM_SERIAL_NUM="FCW2215A1AM"
MOTHERBOARD_SERIAL_NUM="FOC22141LY6"
MOTHERBOARD_REVISION_NUM="B0"
MOTHERBOARD_ASSEMBLY_NUM="73-18140-03"
MODEL_REVISION_NUM="C0"
BAUD="115200"
DC_COPY="yes"
SWITCH_NUMBER="1"
SWITCH_PRIORITY="15"
MAC_ADDR="00:01:02:02:aa:bb"
TAG_ID="E20034120131FB00098B2957"
ENABLE_BREAK="yes"
TEMPLATE="distribution"
TFTP_BLKSIZE="8192"
VERSION_ID="V01"
CRASHINFO="crashinfo:crashinfo_RP_00_00_20180704-001727-UTC"
TFTP_SERVER="10.8.0.6"
BOOT="flash:packages.conf;"
AUTOREBOOT_RESTORE="0"
D_STACK_DAD="""""""""""""""""""""""""""
LICENSE_BOOT_LEVEL="network-essentials+dna-essentials,all:C9500_40X;"
MANUAL_BOOT="yes"
RET_2_RTS=""""""""""""""""""""""""""
ABNORMAL_RESET_COUNT="1"
IP_ADDRESS="10.8.40.173"
IP_SUBNET_MASK="255.255.0.0"
DEFAULT_GATEWAY="10.8.0.1"
ROMMON_AUTOREBOOT_ATTEMPT="3"
BSI="0"
RET_2_RCALTS=""""""""""""""""""""""""""
RANDOM_NUM="1494148250"
```
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**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Control Plane Entries: 512
Input Netflow flows: 8192
Output Netflow flows: 16384
SGT/DGT entries: 4096
SGT/DGT Overflow entries: 512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
**show tech-support license**

To display the debug output, use the `show license tech support` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Example**

This example shows a sample output from the `show tech-support license` command:

```
Device# show tech-support license

------------------ show clock ------------------
*12:35:48.561 EDT Tue Jul 17 2018

------------------ show version ------------------
Cisco IOS XE Software, Version 16.09.01prd7
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K IOSXE), Version 16.9.1prd7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Tue 10-Jul-18 08:47 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license all</td>
<td>Displays entitlements information.</td>
</tr>
<tr>
<td>show license status</td>
<td>Displays compliance status of a license.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays summary of all active licenses.</td>
</tr>
<tr>
<td>show license udi</td>
<td>Displays UDI.</td>
</tr>
<tr>
<td>show license usage</td>
<td>Displays license usage information</td>
</tr>
</tbody>
</table>
**show tech-support platform**

To display detailed information about a platform for use by technical support, use the `show tech-support platform` command in privileged EXEC mode.

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command is used for platform-specific debugging. The output provides detailed information about a platform, such as CPU usage, Ternary Content Addressable Memory (TCAM) usage, capacity, and memory usage.

The output of the `show tech-support platform` command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support platform | redirect flash:filename`) in the local writable storage file system or remote file system.

The output of the `show tech-support platform` command displays a list commands and their output. These commands may differ based on the platform.

**Examples**

The following is sample output from the `show tech-support platform` command:

```
Device# show tech-support platform
.
.
------------------ show platform hardware capacity ------------------
Load Average
Slot Status     1-Min  5-Min 15-Min
1-RP0 Healthy   0.25   0.17  0.12

Memory (kB)
Slot Status     Total    Used (Pct)  Free (Pct) Committed (Pct)
1-RP0 Healthy   3964428 2212476 (56%) 1751952 (44%) 3420472 (86%)

CPU Utilization
Slot  CPU  User  System  Nice  Idle  IRQ  SIRQ  IOwait
1-RP0 0 1.40  0.90  0.00  97.60  0.00  0.10  0.00
  1  2.00  0.20  0.00  97.79  0.00  0.00  0.00
  2  0.20  0.00  0.00  99.80  0.00  0.00  0.00
  3  0.79  0.19  0.00  99.00  0.00  0.00  0.00
  4  5.61  0.50  0.00  93.88  0.00  0.00  0.00
  5  2.90  0.40  0.00  96.70  0.00  0.00  0.00

*: interface is up
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>INQ</th>
<th>IQD</th>
<th>OHQ</th>
<th>OQD</th>
<th>RXBS</th>
<th>RXPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vlan1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet0/0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/21</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/22</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>GigabitEthernet1/0/25</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
show tech-support platform

GigabitEthernet1/0/26 0 0 0 0 0 0 0
GigabitEthernet1/0/27 0 0 0 0 0 0 0
GigabitEthernet1/0/28 0 0 0 0 0 0 0
GigabitEthernet1/0/29 0 0 0 0 0 0 0
GigabitEthernet1/0/30 0 0 0 0 0 0 0
GigabitEthernet1/0/31 0 0 0 0 0 0 0
GigabitEthernet1/0/32 0 0 0 0 0 0 0
GigabitEthernet1/0/33 0 0 0 0 0 0 0
GigabitEthernet1/0/34 0 0 0 0 0 0 0
GigabitEthernet1/0/35 0 0 0 0 0 0 0
GigabitEthernet1/0/36 0 0 0 0 0 0 0
Te1/0/37 0 0 0 0 0 0 0
Te1/0/38 0 0 0 0 0 0 0
Te1/0/39 0 0 0 0 0 0 0
Te1/0/40 0 0 0 0 0 0 0
Te1/0/41 0 0 0 0 0 0 0
Te1/0/42 0 0 0 0 0 0 0
Te1/0/43 0 0 0 0 0 0 0
Te1/0/44 0 0 0 0 0 0 0
Te1/0/45 0 0 0 0 0 0 0
Te1/0/46 0 0 0 0 0 0 0
Te1/0/47 0 0 0 0 0 0 0
Te1/0/48 0 0 0 0 0 0 0
Te1/1/1 0 0 0 0 0 0 0
Te1/1/2 0 0 0 0 0 0 0
Te1/1/3 0 0 0 0 0 0 0
Te1/1/4 0 0 0 0 0 0 0
ASIC 0 Info
-------------
ASIC 0 HASH Table 0 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info: FSE 1
MAB 0: L3 Multicast entries srip 2 3
MAB 1: L3 Multicast entries srip 2 3
MAB 2: SGT_DGT  srip 0 1
MAB 3: SGT_DGT  srip 0 1
MAB 4: (null)  srip
MAB 5: (null)  srip
MAB 6: (null)  srip
MAB 7: (null)  srip

Output fields are self-explanatory.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tech-support platform evpn_vxlan</td>
<td>Displays EVPN-VXLAN-related platform information.</td>
</tr>
<tr>
<td>show tech-support platform fabric</td>
<td>Displays detailed information about the switch fabric.</td>
</tr>
<tr>
<td>show tech-support platform igmp_snooping</td>
<td>Displays IGMP snooping information about a group.</td>
</tr>
<tr>
<td>show tech-support platform layer3</td>
<td>Displays Layer 3 platform forwarding information.</td>
</tr>
<tr>
<td>show tech-support platform mld_snooping</td>
<td>Displays MLD snooping information about a group.</td>
</tr>
</tbody>
</table>
show tech-support platform evpn_vxlan

To display Ethernet VPN (EVPN)-Virtual eXtensible LAN (VXLAN)-related platform information for use by technical support, use the `show tech-support platform evpn_vxlan` command in privileged EXEC mode.

`show tech-support platform evpn_vxlan switch switch-number`

**Syntax Description**

```
switch switch-number
```

Displays information for the specified switch. Valid values are from 1 to 9.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support platform evpn_vxlan switch 1 | redirect flash:filename`) in the local writable storage file system or remote file system.

**Examples**

The following is sample output from the `show tech-support platform evpn_vxlan` command:

```
Device# show tech-support platform evpn_vxlan switch 1

            "show clock"
            "show version"
            "show running-config" switch no: 1

----- sh adm prefer -----  
Showing SDM Template Info

This is the Advanced template.  
Number of VLANs: 4094  
Unicast MAC addresses: 32768  
Overflow Unicast MAC addresses: 512  
L2 Multicast entries: 4096  
Overflow L2 Multicast entries: 512  
L3 Multicast entries: 4096  
Overflow L3 Multicast entries: 512  
Directly connected routes: 16384  
Indirect routes: 7168  
STP Instances: 4096  
Security Access Control Entries: 3072  
QoS Access Control Entries: 2560  
Policy Based Routing ACEs: 1024  
Netflow ACEs: 768  
Flow SPAN ACEs: 512  
Tunnels: 256  
LISP Instance Mapping Entries: 256  
Control Plane Entries: 512
```
Input Netflow flows: 8192
Output Netflow flows: 16384
SGT/DGT (or) MPLS VPN entries: 4096
SGT/DGT (or) MPLS VPN Overflow entries: 512
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 127
MPLS Labels: 2048
MPLS L3 VPN Routes VRF Mode: 7168
MPLS L3 VPN Routes Prefix Mode: 3072
MVFN MDT Tunnels: 256
L2 VPN EOMPLS Attachment Circuit: 256
MAX VPLS Bridge Domains: 64
MAX VPLS Peers Per Bridge Domain: 8
MAX VPLS/VFNS Pseudowires: 256

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. *values can be modified by sdm cli.

----- show platform software fed switch 1 ifm interfaces nve ----- 

----- show platform software fed switch 1 ifm interfaces efp ----- 

----- show platform software fed switch 1 matm macTable ----- 

Total Mac number of addresses: 0
*a_time=aging_time(secs)  e_time=total_elapsed_time(secs)

Type:
  MAT_DYNAMIC_ADDR 0x1 MAT_STATIC_ADDR 0x2 MAT_CPU_ADDR 0x3
  0x4 MAT_DISCARD_ADDR 0x8
  MAT_ALL_VLANs 0x10 MAT_NO_FORWARD 0x20 MAT_IPMULT_ADDR 0x30
  0x40 MAT_RESYNC 0x80
  MAT_DO_NOT безопасности 0x100 MAT_SECURE_ADDR 0x200 MAT_NO_PORT 0x300
  0x400 MAT_DROP_ADDR 0x800
  MAT_DUP_ADDR 0x1000 MAT_NULL_DESTINATION 0x2000 MAT_DOT1X_ADDR 0x3000
  0x4000 MAT_ROUTER_ADDR 0x8000
  MAT_WIRELESS_ADDR 0x100000 MAT_SECURE_CFG_ADDR 0x200000 MAT_OPOQ_DATA_PRESENT 0x300000
  0x400000 MAT_WIRED_TUNNEL_ADDR 0x800000
  MAT_DLR_ADDR 0x10000000 MAT_MRP_ADDR 0x20000000 MAT_MSRP_ADDR 0x30000000
  0x40000000 MAT_LISP_LOCAL_ADDR 0x80000000
  MAT_LISP_REMOTE_ADDR 0x100000000 MAT_VPLS_ADDR 0x200000000

Output fields are self-explanatory.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tech-support platform</td>
<td>Displays detailed information about a platform for use by technical support.</td>
</tr>
</tbody>
</table>
show tech-support platform fabric

To display information about the switch fabric, use the `show tech-support platform fabric` command in privileged EXEC mode.

```
show tech-support platform fabric [display-cli | vrf vrf-name ipv4 display-cli | ipv6 display-cli | source instance-id instance-id ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac mac-address] |
{dest instance-id instance-id} {ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac mac-address} |
{display-cli}]
```

**Syntax Description**

- `display-cli` (Optional) Displays the list of show commands available in the output of this command.
- `vrf vrf-name` (Optional) Displays fabric-related information for the specified virtual routing and forwarding (VRF) instance.
- `ipv4 ip-address/ip-prefix` (Optional) Displays fabric-related information for the source or destination IP VRF.
- `ipv6 ipv6-address/ipv6-prefix` (Optional) Displays fabric-related information for the source or destination IPv6 VRF.
- `source` (Optional) Displays fabric-related information for the source VRF.
- `instance-id instance-id` (Optional) Displays information about the endpoint identifier (EID) of the source.
- `mac mac-address` (Optional) Displays fabric-related information for the source and destination MAC VRF for Layer 2 extension deployments.

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support platform fabric | redirect flash:filename`) in the local writable storage file system or remote file system.
The output of this command displays a list commands and their output. These commands may differ based on the platform.

**Examples**

The following is sample output from the `show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4` command:

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id 4098 ipv4 10.1.1.32 dest instance-id 4098 ipv4 10.12.12.32
.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding  eid remote 10.12.12.12-----

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Fwd action</th>
<th>Locator status</th>
<th>bits</th>
<th>enca pid</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.12.12.32/32</td>
<td>encap</td>
<td>0x00000001</td>
<td>N/A</td>
<td>1/576</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwnn]</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ifnums:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>LISP0.4098(78): 192.0.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 path</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>7F44F8E86CE8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 output chain</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E83738</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-----show lisp instance-id 4098 ipv4 map-cache-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Fwd action</th>
<th>Locator status</th>
<th>bits</th>
<th>Encap-IID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.12.12.32/32</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-----show lisp instance-id 4098 ipv4 map-cache detail-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Fwd action</th>
<th>Locator status</th>
<th>bits</th>
<th>Encap-IID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0/0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-----show tech-support platform fabric-----

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
  Last RLOC-probe sent: 02:45:54 (rtt 1ms)

------show lisp instance-id 4098 ipv4 map-cache 10.12.12.12/32------

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
  Last RLOC-probe sent: 02:45:54 (rtt 1ms)

------show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal------

10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
sources: LISP, IPL
feature space:
  Broker: linked, distributed at 1st priority
subblocks:
  SC owned,sourced: LISP remote EID - locator status bits 0x00000001
LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
LISP source path list
  path list 7F44E6C2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    ifnums:
      LISP0.4098(78): 192.0.2.2
    1 path
      path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
        nexthop 192.0.2.2 LISPO.4098, IP midchain out of LISPO.4098, addr 192.0.2.2
        7F44F8E86CE8
  output chain:
    PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
    IP midchain out of LISPO.4098, addr 192.0.2.2 7F44F8E86CE8
    IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
    Dependent covered prefix type LISP, cover 0.0.0.0/0
      2 IPL sources [no flags]
        ifnums:
          LISPO.4098(78): 192.0.2.2
    path list 7F44E6C2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
        nexthop 192.0.2.2 LISPO.4098, IP midchain out of LISPO.4098, addr 192.0.2.2
        7F44F8E86CE8
    output chain:
      PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
      IP midchain out of LISPO.4098, addr 192.0.2.2 7F44F8E86CE8
      IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
switch no: 1

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189 mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0 | i show

------------------ show clock ------------------
------------------ show version ------------------
------------------ show running-config ------------------
------------------ show device-tracking database ------------------
------------------ show lisp site ------------------
------------------ show mac address-table address 00b7.7128.00a0 ------------------
------------------ show ip arp vrf Campus_VN ------------------
Device#

Output fields are self-explanatory.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command</td>
<td>show tech-support platform</td>
<td>Displays detailed information about a platform for use by technical support.</td>
</tr>
</tbody>
</table>
**show tech-support platform igmp_snooping**

To display Internet Group Management Protocol (IGMP) snooping information about a group, use the `show tech-support platform igmp_snooping` command in privileged EXEC mode.

```
show tech-support platform igmp_snooping [Group_ipAddr ipv4-address | [vlan vlan-ID]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group_ipAddr</td>
<td>(Optional) Displays snooping information about the specified group address.</td>
</tr>
<tr>
<td>ipv4-address</td>
<td>(Optional) IPv4 address of the group.</td>
</tr>
<tr>
<td>vlan vlan-ID</td>
<td>(Optional) Displays IGMP snooping VLAN information. Valid values are from 1 to 4094.</td>
</tr>
</tbody>
</table>

**Command Modes**

Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

The output of this command is very long. To better manage this output, you can redirect the output to a file (for example, `show tech-support platform igmp_snooping | redirect flash:filename`) in the local writable storage file system or remote file system.

**Examples**

The following is sample output from the `show tech-support platform igmp_snooping` command:

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan

----- show ip igmp snooping groups | i 226.6.6.6 ----- 
5 226.6.6.6 user Gi1/0/8, Gi1/0/27, Gi1/0/28,

----- show ip igmp snooping groups count -------
Total number of groups: 2

----- show ip igmp snooping mrouter -------

Vlan  ports
-----  ----- 
23  Router
24  Router
```

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
----- show ip igmp snooping querier -----

<table>
<thead>
<tr>
<th>Vlan</th>
<th>IP Address</th>
<th>IGMP Version</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>10.1.1.1</td>
<td>v2</td>
<td>Router</td>
</tr>
<tr>
<td>24</td>
<td>10.1.2.1</td>
<td>v2</td>
<td>Router</td>
</tr>
<tr>
<td>25</td>
<td>10.1.3.1</td>
<td>v2</td>
<td>Router</td>
</tr>
</tbody>
</table>

----- show ip igmp snooping vlan 5 -----

Global IGMP Snooping configuration:
---------------------------------------------
IGMP snooping : Enabled
Global PIM Snooping : Disabled
IGMPv3 snooping : 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 5:
-------
IGMP snooping : Enabled
Pim Snooping : Disabled
IGMPv2 immediate leave : Disabled
Explicit host tracking : Enabled
Multicast router learning mode : pim-dvmp
CGMP interoperability mode : IGMP_ONLY
Robustness variable : 2
Last member query count : 2
Last member query interval : 1000

----- show ip igmp snooping groups vlan 5 -----

<table>
<thead>
<tr>
<th>Vlan</th>
<th>Group</th>
<th>Type</th>
<th>Version</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>226.6.6.6</td>
<td>user</td>
<td>G11/0/8, G11/0/27, G11/0/28, G12/0/7, G12/0/8, G12/0/27, G12/0/28</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>238.192.0.1</td>
<td>user</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

----- show platform software fed active ip igmp snooping vlan 5 -----

Vlan 5
-------
IGMPSN Enabled : On
PIMSN Enabled : Off
Flood Mode : Off
I-Mrouter : Off
Oper State : Up
show tech-support platform igmp_snooping

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip igmp snooping</td>
<td>Enables IGMP snooping globally or on an interface.</td>
</tr>
<tr>
<td>show ip igmp snooping</td>
<td>Displays the IGMP snooping configuration of a device.</td>
</tr>
<tr>
<td>show tech-support platform</td>
<td>Displays detailed information about a platform for use by technical support.</td>
</tr>
</tbody>
</table>
show tech-support platform layer3

To display Layer 3 platform forwarding information, use the `show tech-support platform layer3` command in privileged EXEC mode.

```
show tech-support platform layer3 {multicast Group_ipAddr ipv4-address switch switch-number srcIP ipv4-address | unicast {dstIP ipv4-address srcIP ipv4-address | vrf vrf-name destIP ipv4-address srcIP ipv4-address}}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>Displays multicast information.</td>
</tr>
<tr>
<td>Group_ipv6Addr ipv4-address</td>
<td>Displays information about the specified multicast group address.</td>
</tr>
<tr>
<td>switch switch-number</td>
<td>Displays information about the specified switch. Valid values are from 1 to 9.</td>
</tr>
<tr>
<td>srcIP ipv4-address</td>
<td>Displays information about the specified source address.</td>
</tr>
<tr>
<td>unicast</td>
<td>Displays unicast-related information.</td>
</tr>
<tr>
<td>dstIP ipv4-address</td>
<td>Displays information about the specified destination address.</td>
</tr>
<tr>
<td>vrf vrf-name</td>
<td>Displays unicast-related virtual routing and forwarding (VRF) information.</td>
</tr>
</tbody>
</table>

### Command Modes

- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2 | redirect flash:filename`) in the local writable storage file system or remote file system.

### Examples

The following is sample output from the `show tech-support platform layer3 multicast group` command:

```
Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1 switch 1 srcIp 10.10.0.2
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
```
switch no: 1

----- show ip mroute 224.1.1.1 10.10.0.2 -----
<table>
<thead>
<tr>
<th>VRF</th>
<th>Interface</th>
<th>IF ID</th>
<th>PIM Status</th>
<th>State</th>
<th>RI Handle</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>GigabitEthernet1/0/10</td>
<td>0x000000000000005f</td>
<td>enabled</td>
<td></td>
<td>0x0000000000000000010</td>
</tr>
<tr>
<td>0</td>
<td>Vlan20</td>
<td>0x0000000000000060</td>
<td>enabled</td>
<td></td>
<td>0x0000000000000000010</td>
</tr>
</tbody>
</table>

----- show platform software fed switch 1 ip multicast groups summary -----

Multicast Groups database

Mvrf_id: 0 Mroute: (*, 224.0.1.40/32) Flags: C IC
  Htm: 0x00007fb414b23ce8 Si: 0x00007fb414b23a08 Di: 0x00007fb414b240e8 Rep_ri: 0x00007fb414b245f8

Mvrf_id: 0 Mroute: (*, 224.0.0.0/4) Flags: C
  Htm: 0x00007fb4143549e8 Si: 0x00007fb414b20a48 Di: 0x00007fb414b1fe78 Rep_ri: 0x00007fb414b20428

Mvrf_id: 0 Mroute: (*)(224.1.1.1/32) Flags: C IC
  Htm: 0x00007fb414b2cc98 Si: 0x00007fb414b2678 Di: 0x00007fb414b2ab98 Rep_ri: 0x00007fb414b2b0c8

Mvrf_id: 0 Mroute: (10.10.0.2, 224.1.1.1/32) Flags: IC
  Htm: 0x00007fb414b2f348 Si: 0x00007fb414b321d8 Di: 0x00007fb414b2dba8 Rep_ri: 0x00007fb414b30ed8

----- show platform software fed switch 1 ip multicast groups count -----

Total Number of entries: 4

----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32 source 10.10.0.2 detail -----
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00

Destination Index (DI) [0x538e]
portMap = 0x00000000 0
cmi1 = 0x385
rcpPortMap = 0

Detailed Resource Information (ASIC# 0)
----------------------------------------
al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0

Destination Index (DI) [0x538e]
portMap = 0x00000000 0
cmi1 = 0x385
rcpPortMap = 0

Detailed Resource Information (ASIC# 1)
----------------------------------------
al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
cpuQNum0 = 0x9e

RI details
----------
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_r/priv_s/Handle:(nil) Hardware Indices/Rlndexes: index0:0x5 mtu_index/l3u_ri_index0:0x0
index1:0x5 mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Detailed Resource Information (ASIC# 0)
----------------------------------------

Detailed Resource Information (ASIC# 1)
----------------------------------------
SI details
----------
priv_ri/priv_si Handle: (nil) Hardware Indices/Handles: index0: 0x4004 mtu_index/l3u_ri_index0: 0x0 sm_handle 0: 0x7fb414b2df98 index1: 0x4004 mtu_index/l3u_ri_index1: 0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------
Detailed Resource Information (ASIC# 1)
----------------------------------------

HTM details
----------
Handle: 0x7fb414b2f348 Res-Type: ASIC_RSC_HASH_TCAM Res-Switch-Num: 0 Asic-Num: 255 Feature-ID: AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id: LKP_FEAT_IPV4_MCAST_SG ref_count: 1
priv_ri/priv_si Handle: (nil) Hardware Indices/Handles: handle0: 0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1
Entry #0: (handle 0x7fb414b2f558)
KEY - src_addr: 10.10.0.2 starg_station_index: 16387
MASK - src_addr: 0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr: 0
afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index: 0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

The following is sample output from the show tech-support platform layer3 unicast vrf command:

Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20 srcIP 10.0.0.10
.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name:
Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite
Switch# Role Mac Address Priority Version State
-------------------------------------------------------------------------------------
*1 Active 5006.ab89.0280 1 V02 Ready

----- show switch -----

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
10.0.0.10 -> 10.0.0.20 -> IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20

----- show ip cef  exact-route platform 10.0.0.10 10.0.0.20 ----- 

next hop is 10.0.0.20 

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Interface</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>GigabitEthernet1/0/7</td>
<td>10.0.0.20(8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 packets, 0 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>epoch 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sourced in sev-epoch 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encap length 14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>00211BFDE6495006AB8902C00800</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2 destination address byte offset 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L2 destination address byte length 6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Link-type after encap: ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ARP</td>
</tr>
</tbody>
</table>

----- show adjacency 10.0.0.20 detail ----- 

Routing entry for 10.0.0.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via GigabitEthernet1/0/7
  Route metric is 0, traffic share count is 1

----- show ip route 10.0.0.20 ----- 

10.0.0.20/32, epoch 3, flags [attached]
Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
Dependent covered prefix type adjfib, cover 10.0.0.0/24 attached to GigabitEthernet1/0/7

----- show ip cef  10.0.0.20 detail ----- 

ip prefix: 10.0.0.20/32

Forwarding Table
10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
OM handle: 0x10205416d8

----- show platform software ip switch 1 R0 cef prefix 10.0.0.20/32 detail ----- 

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
OBJ_ADJACENCY found: 29

Number of adjacency objects: 5

Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x1020541348

----- show platform software adjacency switch 1 R0 index 29 -----

Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
  Connected Interface: 31
  Prefix Flags: Directly L2 attached
  aom id: 393, HW handle: (nil) (created)

----- show platform software ip switch 1 F0 cef prefix 10.0.0.20/32 detail -----

OBJ_ADJACENCY found: 29

Number of adjacency objects: 5

Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  aom id: 391, HW handle: (nil) (created)

----- show platform software adjacency switch 1 F0 index 29 -----

found aom id: 391
Object identifier: 391
Description: adj 0x1d, Flags None
Status: Done, Epoch: 0, Client data: 0xc6a747a8

----- show platform software object-manager switch 1 F0 object 391-----

Object identifier: 66
Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM dirty NONE
Status: Done

----- show platform software object-manager switch 1 F0 object 391 parents-----

Object identifier: 393
Description: PREFIX 10.0.0.20/32 (Table id 0)
Status: Done

Output fields are self-explanatory.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show tech-support platform</td>
<td>Displays detailed information about a platform for use by technical support.</td>
</tr>
</tbody>
</table>
show tech-support platform mld_snooping

To display Multicast Listener Discovery (MLD) snooping information about a group, use the show tech-support platform mld_snooping command in privileged EXEC mode.

show tech-support platform mld_snooping [{Group_ipv6Addr ipv6-address }] [ {vlan vlan-ID} ]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group_ipv6Addr</td>
<td>(Optional) Displays snooping information about the specified group address.</td>
</tr>
<tr>
<td>ipv6-address</td>
<td>(Optional) IPv6 address of the group.</td>
</tr>
<tr>
<td>vlan vlan-ID</td>
<td>(Optional) Displays MLD snooping VLAN information. Valid values are from 1 to 4094.</td>
</tr>
</tbody>
</table>

Command Modes

Privileged EXEC (#)

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, show tech-support platform mld_snooping | redirect flash:filename) in the local writable storage file system or remote file system.

Examples

The following is sample output from the show tech-support platform mld_snooping command:

Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1

. .
.------------------ show running-config ------------------

Building configuration...

Current configuration : 11419 bytes

! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
! version 16.10
! no service pad
! service timestamps debug datetime msec
! service timestamps log datetime msec
! service call-home
! no platform punt-keepalive disable-kernel-core
! hostname Switch
! vrf definition Mgmt-vrf
! address-family ipv4
! exit-address-family
!
! address-family ipv6
! exit-address-family
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "profile-1"
  active
  destination transport-method http
  no destination transport-method email
  
  ip admission watch-list expiry-time 0
  
  login on-success log
  
  
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed=559433368
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate=559433368
  revocation-check none
  rsakeypair TP-self-signed=559433368
!
crypto pki trustpoint SLA-TrustPoint
  enrollment pkcs12
  revocation-check crl
!
crypto pki certificate chain TP-self-signed=559433368
  certificate self-signed 01
    30820229 30820192 A0030201 02020101 02000000 2A864886 F70D0101 05050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D5369676E65642D 43657274
    6963617465 2D35353934 33333638 019F3000 06092A86 4886F70D 01010105 0003818D
    00300000 5A300012 2E305269 6271746F 6375732F 70726F 6F62312E 3030818D 02818100
    AD8C9C3B FE77FC8 986837D2 4C126172 446C3C53 E040F798 4BA6AC79 75006FDCE
    46365DDA E473F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8315F 0B8669CF6
    AA5B5C6C FC2E02F6 FE08B17F 0164FC79 70C84ABB C99D91D6 0B8233FF 814EF6DA
    6DC8FC20 CA12CD65 1CB28EDE 6ADD6DFA 7E3E8281 4A1809A9A AA44FCC0 BA0BD8A5
    02030100 01A35300 51300006 005551B3 01010004 05030001 01FF301F 0603551D
crypto pki certificate chain SLA-TrustPoint

certificate ca 01

quit

Command Reference, Cisco IOS XE Gibraltar 16.12.x (Catalyst 9500 Switches)
DATA, RPF Failed

```bash
class-map match-any AutoQos-4.0-RT1-Class
  match dscp ef
  match dscp cs6
class-map match-any system-cpp-police-punt-webauth
description Punt Webauth
class-map match-any AutoQos-4.0-RT2-Class
  match dscp cs4
  match dscp cs3
  match dscp af41
class-map match-any system-cpp-police-l2lvx-control
description L2 LVX control packets
class-map match-any system-cpp-police-forus
description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
description MCAST END STATION
class-map match-any system-cpp-police-multicast
description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
description L2 control
class-map match-any system-cpp-police-dot1x-auth
description DOT1X Auth
class-map match-any system-cpp-police-data
description ICMP redirect, ICMP GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
description Stackwise Virtual
class-map match-any system-cpp-police-control-low-priority
description ICMP redirect and general punt
class-map match-any system-cpp-police-wireless-priority1
description Wireless priority 1
class-map match-any system-cpp-police-wireless-priority2
description Wireless priority 2
class-map match-any system-cpp-police-wireless-priority3-4-5
description Wireless priority 3,4 and 5
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
description DHCP snooping
class-map match-any system-cpp-police-system-critical
description System Critical and Gold Pkt
```

```bash
policy-map system-cpp-policy
class system-cpp-police-data
police rate 200 pps
class system-cpp-police-routing-control
police rate 500 pps
class system-cpp-police-control-low-priority
class system-cpp-police-wireless-priority1
class system-cpp-police-wireless-priority2
class system-cpp-police-wireless-priority3-4-5
policy-map port_child_policy
class non-client-nrt-class
  bandwidth remaining ratio 10
  ```
interface GigabitEthernet0/0
  vrf forwarding Mgmt-vrf
  no ip address
  speed 1000
  negotiation auto
interface GigabitEthernet1/0/1
  switchport mode access
  macsec network-link
interface GigabitEthernet1/0/2
interface GigabitEthernet1/0/3
interface TenGigabitEthernet1/1/1
interface TenGigabitEthernet1/1/2
interface TenGigabitEthernet1/1/3
interface TenGigabitEthernet1/1/4
interface Vlan1
  no ip address
  shutdown
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data
  permit tcp any any eq 22
  permit tcp any any eq 465
  permit tcp any any eq 143
  permit tcp any any eq 993
  permit tcp any any eq 995
  permit tcp any any eq 1914
  permit tcp any any eq ftp
  permit tcp any any eq ftp-data
  permit tcp any any eq smtp
  permit tcp any any eq pop3
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf
  permit udp any any range 16384 32767
  permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-wlan-Acl-Scavanger
  permit tcp any any range 2300 2400
  permit udp any any range 2300 2400
  permit tcp any any range 6881 6999
  permit tcp any any range 28800 29100
  permit tcp any any eq 1214
  permit udp any any eq 1214
  permit tcp any any eq 3689
  permit udp any any eq 3689
  permit tcp any any eq 11999
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling
  permit tcp any any range 2000 2002
  permit tcp any any range 5060 5061
  permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
  permit tcp any any eq 443
  permit tcp any any eq 1521
permit udp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1630
permit tcp any any eq 1527
permit tcp any any eq 6200
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
!
!
ipv6 access-list preauth_ipv6_acl
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
service-policy input system-cpp-policy
!
line con 0
    stopbits 1
line aux 0
    stopbits 1
line vty 0 4
    login
line vty 5 15
    login
!
mac address-table notification mac-move
!
!
!
end

-----show switch | Include Ready-----
*1 Active 188b.9dfc.eb00 1 V00 Ready

----- show ipv6 mld snooping address | i FF02::5:1 -----
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ipv6 mld snooping</code></td>
<td>Enables MLDv2 protocol snooping globally.</td>
</tr>
<tr>
<td><code>show ipv6 mld snooping</code></td>
<td>Displays MLDv2 snooping information.</td>
</tr>
<tr>
<td><code>show tech-support platform</code></td>
<td>Displays detailed information about a platform for use by technical support.</td>
</tr>
</tbody>
</table>
show tech-support port

To display port-related information for use by technical support, use the `show tech-support port` command in privileged EXEC mode.

```
show tech-support port
```

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

**Command Modes**
Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The output of the `show tech-support port` command is very long. To better manage this output, you can redirect the output to an external file (for example, `show tech-support port | redirect flash:filename`) in the local writable storage file system or remote file system.

The output of this command displays the following commands:

- `show clock`
- `show version`
- `show module`
- `show inventory`
- `show interface status`
- `show interface counters`
- `show interface counters errors`
- `show interfaces`
- `show interfaces capabilities`
- `show controllers`
- `show controllers utilization`
- `show idprom interface`
- `show controller ethernet-controller phy detail`
- `show switch`
- `show platform software fed switch active port summary`
- `show platform software fed switch ifm interfaces ethernet`
- `show platform software fed switch ifm mappings`
- `show platform software fed switch ifm mappings lpn`
Examples

The following is sample output from the `show tech-support port` command:

```
Device# show tech-support port

----- show controllers utilization -----

<table>
<thead>
<tr>
<th>Port</th>
<th>Receive Utilization</th>
<th>Transmit Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/7</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/8</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/10</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/11</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/13</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/15</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/16</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/17</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/18</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/19</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/20</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/21</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/22</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/23</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/24</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/25</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/26</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/27</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/28</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/29</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/30</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/31</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/32</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/33</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/34</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/35</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/36</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/37</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/38</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/39</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/40</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/41</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/42</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/43</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Te1/0/44</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
### Total Ports:
Total Ports : 52

### Bandwidth Percentage Utilization:
- Total Ports Receive Bandwidth Percentage Utilization : 0
- Total Ports Transmit Bandwidth Percentage Utilization : 0

### Average Switch Percentage Utilization:
Average Switch Percentage Utilization : 0

**----- show idprom interface Gi1/0/1 -----**

*Sep 7 08:57:24.249: No module is present
.
.
.

The output fields are self-explanatory.
show version

To display information about the currently loaded software along with hardware and device information, use the show version command in user EXEC or privileged EXEC mode.

```
show version [switch node] [installed | provisioned | running]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>switch node</td>
<td>(optional) Only a single switch may be specified. Default is all switches in a stacked system.</td>
</tr>
<tr>
<td>running</td>
<td>(optional) Specifies information on the files currently running.</td>
</tr>
<tr>
<td>provisioned</td>
<td>(optional) Specifies information on the software files that are provisioned.</td>
</tr>
<tr>
<td>installed</td>
<td>Specifies information on the software installed on the RP</td>
</tr>
<tr>
<td>user-interface</td>
<td>Specifies information on the files related to the user-interface.</td>
</tr>
</tbody>
</table>

### Command Default

No default behavior or values.

### Command Modes

- User EXEC (>)
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

This command displays information about the Cisco IOS software version currently running on a device, the ROM Monitor and Bootflash software versions, and information about the hardware configuration, including the amount of system memory. Because this command displays both software and hardware information, the output of this command is the same as the output of the show hardware command. (The show hardware command is a command alias for the show version command.)

Specifically, the show version command provides the following information:

- **Software information**
  - Main Cisco IOS image version
  - Main Cisco IOS image capabilities (feature set)
  - Location and name of bootfile in ROM
  - Bootflash image version (depending on platform)

- **Device-specific information**
  - Device name
  - System uptime
  - System reload reason
  - Config-register setting
  - Config-register settings for after the next reload (depending on platform)
- Hardware information
  - Platform type
  - Processor type
  - Processor hardware revision
  - Amount of main (processor) memory installed
  - Amount I/O memory installed
  - Amount of Flash memory installed on different types (depending on platform)
  - Processor board ID

The output of this command uses the following format:

Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>, <software-type>
Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>
ROM: System Bootstrap, Version <software-version>, <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>, <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours, <m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform><processor-revision-id> processor (revision <processor-revision-id>) with <free-DRAM-memory> K/<packet-memory> K bytes of memory.
Processor board ID <ID-number>

CPU type <CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache

See the Examples section for descriptions of the fields in this output.

Entering `show version` displays the IOS XE software version and the IOS XE software bundle which includes a set of individual packages that comprise the complete set of software that runs on the switch.

The `show version running` command displays the list of individual packages that are currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the bundle.

The `show version provisioned` command displays information about the provisioned package set.

The following is sample output from the `show version` command on a Cisco Catalyst 9300 Series Switch:

```
Device# show version
Cisco IOS XE Software, Version BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2
Cisco IOS Software (Fuji), Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version 16.10.20180903:072347
{v1610_throttle-/nobackup/mcpre/BLD-BLD_V1610_THROTTLE_LATEST_20180903_070602 183}
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 03-Sep-18 11:53 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
```
show version

All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)

C9300 uptime is 20 hours, 7 minutes
Uptime for this control processor is 20 hours, 8 minutes
System returned to ROM by Image Install
System image file is "flash:packages.conf"
Last reload reason: Image Install

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

A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.

Technology Package License Information:

<table>
<thead>
<tr>
<th>Technology-package</th>
<th>Current Type</th>
<th>Next reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-advantage</td>
<td>Smart License</td>
<td>network-advantage</td>
</tr>
<tr>
<td>dna-advantage</td>
<td>Subscription Smart License</td>
<td>dna-advantage</td>
</tr>
</tbody>
</table>

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.
Processor board ID FCWZ125LUBH
8 Virtual Ethernet interfaces
56 Gigabit Ethernet interfaces
16 Ten Gigabit Ethernet interfaces
4 TwentyFive Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:
1638400K bytes of Crash Files at crashinfo-2:
11264000K bytes of Flash at flash:
11264000K bytes of Flash at flash-2:
0K bytes of WebUI ODM Files at webui:
In the following example, the `show version running` command is entered on a Cisco Catalyst 9300 Series Switch to view information about the packages currently running on both switches in a 2-member stack:

```
Device# show version running
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: active
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpree
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: active
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpree
  File SHA1 checksum: n/a

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: active
  Role: guestshell
  File: /flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0/0
```
In the following example, the `show version provisioned` command is entered on a Cisco Catalyst 9300 Series Switch that is the active switch in a 2-member stack. The `show version provisioned` command displays information about the packages in the provisioned package set.

```
Device# show version provisioned
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5
```
show version

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: guestshell
  File: /flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d1a926acc6be05414408d7

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_ioad
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6e1bfb266ad7eb553a

Package: wlc, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
  Role: rp_wlc
  File: /flash/cat9k-wlc.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
  Built: 2018-09-03_13.11, by: mcpre
Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
Role: srdriver
File: /flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: RP0
   Built: 2018-09-03_13.11, by: mcpre
   File SHA1 checksum: aff411e981a8dfc8de1405cc33462dc69f8baf

Package: espbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
Role: fp
File: /flash/cat9k-espbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: ESP0
   Built: 2018-09-03_13.11, by: mcpre
   File SHA1 checksum: 1a2317485f285a3945b31ae57aa6c56ed30a8c0

Package: sipbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
Role: cc
File: /flash/cat9k-sipbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: SIP0
   Built: 2018-09-03_13.11, by: mcpre
   File SHA1 checksum: ce821195f6c0bd5e44f21e32fca76cf9b2ed0b

Package: sipspa, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
Role: cc_spa
File: /flash/cat9k-sipspa.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: SIP0
   Built: 2018-09-03_13.11, by: mcpre
   File SHA1 checksum: 54645404860b662d72f8ff7fa5e6e88cb0960e20

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status: n/a
Role: cc_srdriver
File: /flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on: SIP0
   Built: 2018-09-03_13.11, by: mcpre
   File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7

**Table 170: Table 5, show version running Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Package</td>
<td>The individual sub-package name.</td>
</tr>
<tr>
<td>version</td>
<td>The individual sub-package version.</td>
</tr>
<tr>
<td>status</td>
<td>Reveals if the package is active or inactive for the specific Supervisor module.</td>
</tr>
<tr>
<td>File</td>
<td>The filename of the individual package file.</td>
</tr>
<tr>
<td>on</td>
<td>The slot number of the Active or Standby Supervisor that this package is running on.</td>
</tr>
<tr>
<td>Built</td>
<td>The date the individual package was built.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Device</th>
<th>Difference between Yellow and Red</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 9500</td>
<td>14°C</td>
<td>60°C</td>
</tr>
</tbody>
</table>

* You cannot configure the red temperature threshold.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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)#
```
**traceroute mac**

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the `traceroute mac` command in privileged EXEC mode.

```
traceroute mac [interface interface-id] source-mac-address [interface interface-id] destination-mac-address [vlan vlan-id] [detail]
```

**Syntax Description**

- `interface interface-id` (Optional) Specifies an interface on the source or destination device.
- `source-mac-address` The MAC address of the source device in hexadecimal format.
- `destination-mac-address` The MAC address of the destination device in hexadecimal format.
- `vlan vlan-id` (Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
- `detail` (Optional) Specifies that detailed information appears.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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) :G10/0/1 -> G10/0/3
con5 (2.2.5.5 ) : G10/0/3 -> G10/0/1
con1 (2.2.1.1 ) : G10/0/1 -> G10/0/2
con2 (2.2.2.2 ) : G10/0/2 -> G10/0/1
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 :
   G10/0/2 [auto, auto] => G10/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
   Fa0/3 [auto, auto] => G10/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
   G10/1 [auto, auto] => G10/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
   G10/2 [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) :G10/0/1 -> G10/0/3
con5 (2.2.5.5 ) : G10/0/3 -> G10/0/1
con1 (2.2.1.1 ) : G10/0/1 -> G10/0/2
con2 (2.2.2.2 ) : G10/0/2 -> G10/0/1
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 :
   G10/0/1 [auto, auto] => G10/0/3 [auto, auto]
```
This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error: Source Mac address not found.
  Layer 2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error: Source and destination macs are on different vlans.
  Layer 2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error: Mac found on multiple vlans.
  Layer 2 trace aborted.
```
traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the traceroute mac ip command in privileged EXEC mode.

```
traceroute mac ip {source-ip-address source-hostname} {destination-ip-address destination-hostname} [detail]
```

**Syntax Description**

- **source-ip-address**: The IP address of the source device as a 32-bit quantity in dotted-decimal format.
- **source-hostname**: The IP hostname of the source device.
- **destination-ip-address**: The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
- **destination-hostname**: The IP hostname of the destination device.
- **detail**: (Optional) Specifies that detailed information appears.

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The traceroute mac ip command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.
This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the `detail` keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac ......
2.2.66.66  ->  0000.0201.0601
2.2.22.22  ->  0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
  Gi0/0/1 [auto, auto] -> Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
con1 / WS-C3550-12G / 2.2.1.1 :
  Gi0/1 [auto, auto] -> Gi0/0/3 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
  Gi0/2 [auto, auto] -> Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac ......
2.2.66.66  ->  0000.0201.0601
2.2.22.22  ->  0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) : Gi0/0/1 -> Gi0/0/3
con5 (2.2.5.5  ) : Gi0/0/3 -> Gi0/1
con1 (2.2.1.1  ) : Gi0/0/1 -> Gi0/2
con2 (2.2.2.2  ) : Gi0/0/2 -> Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```
type

To display the contents of one or more files, use the **type** command in boot loader mode.

**type filesystem:/file-url...**

**Syntax Description**

- **filesystem**: Alias for a file system. Use **flash**: for the system board flash device; use **usbflash0**: for USB memory sticks.
- **/file-url...**: Path (directory) and name of the files to display. Separate each filename with a space.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appear sequentially.

**Examples**

This example shows how to display the contents of a file:

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```
To reset one or more environment variables, use the `unset` command in boot loader mode.

`unset` variable...

**Syntax Description**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>MANUAL_BOOT</code></td>
<td>Specifies whether the device automatically or manually boots.</td>
</tr>
<tr>
<td><code>BOOT</code></td>
<td>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: filesystem. 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.</td>
</tr>
<tr>
<td><code>ENABLE_BREAK</code></td>
<td>Specifies whether the automatic boot process can be interrupted by using the <code>Break</code> key on the console after the flash: file system has been initialized.</td>
</tr>
<tr>
<td><code>HELPER</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>PS1</code></td>
<td>Specifies the string that is used as the command-line prompt in boot loader mode.</td>
</tr>
<tr>
<td><code>CONFIG_FILE</code></td>
<td>Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</td>
</tr>
<tr>
<td><code>BAUD</code></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**
This example shows how to display the boot loader version on a device:
Tracing

- Information About Tracing, on page 1536
- set platform software trace, on page 1538
- show platform software trace filter-binary, on page 1542
- show platform software trace message, on page 1543
- show platform software trace level, on page 1546
- request platform software trace archive, on page 1549
- request platform software trace rotate all, on page 1550
- request platform software trace filter-binary, on page 1551
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>
<thead>
<tr>
<th>Tracing Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency</td>
<td>The message is regarding an issue that makes the system unusable.</td>
</tr>
<tr>
<td>Error</td>
<td>The message is regarding a system error.</td>
</tr>
<tr>
<td>Warning</td>
<td>The message is regarding a system warning.</td>
</tr>
<tr>
<td>Notice</td>
<td>The message is regarding a significant issue, but the switch is still working normally.</td>
</tr>
<tr>
<td>Informational</td>
<td>The message is useful for informational purposes only.</td>
</tr>
<tr>
<td>Debug</td>
<td>The message provides debug-level output.</td>
</tr>
<tr>
<td>Verbose</td>
<td>All possible trace messages are sent.</td>
</tr>
<tr>
<td>Noise</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.
**slot**

Hardware slot where the process for which the trace level is set, is running. Options include:

- **number**—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.

- **SIP-slot / SPA-bay**—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.

- **F0**—The Embedded-Service-Processor in slot 0.

- **FP active**—The active Embedded-Service-Processor.

- **R0**—The route processor in slot 0.

- **RP active**—The active route processor.

- **switch <number>**—The switch with its number specified.

- **switch active**—The active switch.

- **switch standby**—The standby switch.

---

**module**

Module within the process for which the tracing level is set.
set platform software trace

**Trace level**

<table>
<thead>
<tr>
<th>trace-level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug</td>
<td>Debug level tracing. A debug-level trace message is a non-urgent message providing a large amount of detail about the module.</td>
</tr>
<tr>
<td>emergency</td>
<td>Emergency level tracing. An emergency-level trace message is a message indicating that the system is unusable.</td>
</tr>
<tr>
<td>error</td>
<td>Error level tracing. An error-level tracing message is a message indicating a system error.</td>
</tr>
<tr>
<td>info</td>
<td>Information level tracing. An information-level tracing message is a non-urgent message providing information about the system.</td>
</tr>
<tr>
<td>noise</td>
<td>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.</td>
</tr>
<tr>
<td>notice</td>
<td>The message is regarding a significant issue, but the switch is still working normally.</td>
</tr>
<tr>
<td>verbose</td>
<td>Verbose level tracing. All possible tracing messages are sent when the trace level is set to verbose.</td>
</tr>
<tr>
<td>warning</td>
<td>Warning messages.</td>
</tr>
</tbody>
</table>

**Command Default**
The default tracing level for all modules is **notice**.

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

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

Syntax Description

```
context mac-address
```

- **context**
  - 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- This command collates and sorts all the logs present in the `/tmp/.../` across all the processes relevant to the module. The trace logs of all the processes relevant to the specified module are printed to the console. This command also generates a file named `collated_log_{system time}` with the same content, in the `/crashinfo/tracelogs` directory.
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**

<table>
<thead>
<tr>
<th>process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracing level that is being set. Options include:</td>
</tr>
<tr>
<td>• <strong>chassis-manager</strong> — The Chassis Manager process.</td>
</tr>
<tr>
<td>• <strong>cli-agent</strong> — The CLI Agent process.</td>
</tr>
<tr>
<td>• <strong>cmm</strong> — The CMM process.</td>
</tr>
<tr>
<td>• <strong>dbm</strong> — The Database Manager process.</td>
</tr>
<tr>
<td>• <strong>emd</strong> — The Environmental Monitoring process.</td>
</tr>
<tr>
<td>• <strong>fed</strong> — The Forwarding Engine Driver process.</td>
</tr>
<tr>
<td>• <strong>forwarding-manager</strong> — The Forwarding Manager process.</td>
</tr>
<tr>
<td>• <strong>geo</strong> — The Geo Manager process.</td>
</tr>
<tr>
<td>• <strong>host-manager</strong> — The Host Manager process.</td>
</tr>
<tr>
<td>• <strong>interface-manager</strong> — The Interface Manager process.</td>
</tr>
<tr>
<td>• <strong>iomd</strong> — The Input/Output Module daemon (IOMd) process.</td>
</tr>
<tr>
<td>• <strong>ios</strong> — The IOS process.</td>
</tr>
<tr>
<td>• <strong>license-manager</strong> — The License Manager process.</td>
</tr>
<tr>
<td>• <strong>logger</strong> — The Logging Manager process.</td>
</tr>
<tr>
<td>• <strong>platform-mgr</strong> — The Platform Manager process.</td>
</tr>
<tr>
<td>• <strong>pluggable-services</strong> — The Pluggable Services process.</td>
</tr>
<tr>
<td>• <strong>replication-mgr</strong> — The Replication Manager process.</td>
</tr>
<tr>
<td>• <strong>shell-manager</strong> — The Shell Manager process.</td>
</tr>
<tr>
<td>• <strong>sif</strong> — The Stack Interface (SIF) Manager process.</td>
</tr>
<tr>
<td>• <strong>smd</strong> — The Session Manager process.</td>
</tr>
<tr>
<td>• <strong>stack-mgr</strong> — The Stack Manager process.</td>
</tr>
<tr>
<td>• <strong>table-manager</strong> — The Table Manager Server.</td>
</tr>
<tr>
<td>• <strong>thread-test</strong> — The Multithread Manager process.</td>
</tr>
<tr>
<td>• <strong>virt-manager</strong> — The Virtualization Manager process.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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]
10/29 13:28:19.023 [stack_mgr] [8974]: (note): Examining peer state 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 expired
10/29 13:26:46.584 [btrace] [8974]: (note): Successfully registered module [99]
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 13:26:36.581 [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**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>process</th>
<th>Process whose tracing level is being set. Options include:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• <strong>chassis-manager</strong> — The Chassis Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>cli-agent</strong> — The CLI Agent process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>cmm</strong> — The CMM process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>dbm</strong> — The Database Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>emd</strong> — The Environmental Monitoring process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>fed</strong> — The Forwarding Engine Driver process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>forwarding-manager</strong> — The Forwarding Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>geo</strong> — The Geo Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>host-manager</strong> — The Host Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>interface-manager</strong> — The Interface Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>iomd</strong> — The Input/Output Module daemon (IOMd) process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>ios</strong> — The IOS process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>license-manager</strong> — The License Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>logger</strong> — The Logging Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>platform-mgr</strong> — The Platform Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>pluggable-services</strong> — The Pluggable Services process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>replication-mgr</strong> — The Replication Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>shell-manager</strong> — The Shell Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>sif</strong> — The Stack Interface (SIF) Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>smd</strong> — The Session Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>stack-mgr</strong> — The Stack Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>table-manager</strong> — The Table Manager Server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>thread-test</strong> — The Multithread Manager process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>virt-manager</strong> — The Virtualization Manager process.</td>
</tr>
</tbody>
</table>
**show platform software trace level**

Hardware slot where the process for which the trace level is set, is running. Options include:

- **number**—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.

- **SIP-slot / SPA-bay**—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.

- **F0**—The Embedded Service Processor in slot 0.

- **F1**—The Embedded Service Processor in slot 1.

- **FP active**—The active Embedded Service Processor.

- **R0**—The route processor in slot 0.

- **RP active**—The active route processor.

- **switch** <number>—The switch, with its number specified.

- **switch active**—The active switch.

- **switch standby**—The standby switch.

  - **number**—Number of the SIP slot of the hardware module where the trace level is set. For instance, if you want to specify the SIP in SIP slot 2 of the switch, enter 2.

  - **SIP-slot / SPA-bay**—Number of the SIP switch slot and the number of the shared port adapter (SPA) bay of that SIP. For instance, if you want to specify the SPA in bay 2 of the SIP in switch slot 3, enter 3/2.

  - **F0**—The Embedded Service Processor in slot 0.

  - **FP active**—The active Embedded Service Processor.

  - **R0**—The route processor in slot 0.

  - **RP active**—The active route processor.

---

**Command Modes**

- User EXEC (>)
- Privileged EXEC (#)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to view the trace level:

```
Device# show platform software trace level dbm switch active R0
```
<table>
<thead>
<tr>
<th>Module Name</th>
<th>Trace Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>bins</td>
<td>Notice</td>
</tr>
<tr>
<td>bins/brand</td>
<td>Notice</td>
</tr>
<tr>
<td>bipc</td>
<td>Notice</td>
</tr>
<tr>
<td>btrace</td>
<td>Notice</td>
</tr>
<tr>
<td>bump_ptr_alloc</td>
<td>Notice</td>
</tr>
<tr>
<td>cdllib</td>
<td>Notice</td>
</tr>
<tr>
<td>chasfs</td>
<td>Notice</td>
</tr>
<tr>
<td>dbal</td>
<td>Informational</td>
</tr>
<tr>
<td>dbm</td>
<td>Debug</td>
</tr>
<tr>
<td>evlib</td>
<td>Notice</td>
</tr>
<tr>
<td>evutil</td>
<td>Notice</td>
</tr>
<tr>
<td>file_alloc</td>
<td>Notice</td>
</tr>
<tr>
<td>green-be</td>
<td>Notice</td>
</tr>
<tr>
<td>ios-avl</td>
<td>Notice</td>
</tr>
<tr>
<td>klib</td>
<td>Debug</td>
</tr>
<tr>
<td>services</td>
<td>Notice</td>
</tr>
<tr>
<td>sw_wdog</td>
<td>Notice</td>
</tr>
<tr>
<td>syshw</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_cdlcore_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_dbal_root_message</td>
<td>Notice</td>
</tr>
<tr>
<td>tdl_dbal_root_type</td>
<td>Notice</td>
</tr>
</tbody>
</table>
request platform software trace archive

To archive all the trace logs relevant to all the processes running on a system since the last reload on the switches and to save this in the specified location, use the `request platform software trace archive` command in privileged EXEC or user EXEC mode.

```
request platform software trace archive [last number-of-days [days [target location] ] ] | target location
```

### Syntax Description

- **last number-of-days**: Specifies the number of days for which the trace files have to be archived.
- **target location**: Specifies the location and name of the archive file.

### Command Modes

- User EXEC (>
- Privileged EXEC (#)

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

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 mac-address** | Represents the context used to filter. Additionally, you can filter based on module names and trace levels. The context keyword accepts either a MAC address or any other argument based on which a trace is tagged. |

<table>
<thead>
<tr>
<th><strong>Command Modes</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC (&gt;)</td>
</tr>
<tr>
<td>Privileged EXEC (#)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Command History</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release</strong></td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Usage Guidelines</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This command collates and sorts all the archived logs present in the tracelogs subdirectory, across all the processes relevant to the module. This command also generates a file named <code>collated_log_{system time}</code> with the same content, in the <code>/crashinfo/tracelogs</code> directory.</td>
</tr>
</tbody>
</table>
request platform software trace filter-binary
PART XIII

VLAN

• VLAN Commands, on page 1555
VLAN Commands

- clear vtp counters, on page 1556
- debug sw-vlan, on page 1557
- debug sw-vlan ifs, on page 1558
- debug sw-vlan notification, on page 1559
- debug sw-vlan vtp, on page 1560
- dot1q vlan native, on page 1562
- interface (VLAN), on page 1563
- private-vlan, on page 1564
- private-vlan mapping, on page 1566
- show dot1q-tunnel, on page 1568
- show interfaces private-vlan mapping, on page 1569
- show vlan, on page 1570
- show vtp, on page 1574
- switchport mode private-vlan, on page 1580
- switchport priority extend, on page 1582
- switchport trunk, on page 1583
- vlan, on page 1586
- vlan dot1q tag native, on page 1592
- vtp (global configuration), on page 1593
- vtp (interface configuration), on page 1598
- vtp primary, on page 1599
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 Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

This example shows how to clear the VTP counters:

```
Device> enable
Device# clear vtp counters
```

You can verify that information was deleted by entering the **show vtp counters** privileged EXEC command.
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 | mapping | notification | packets | redundancy | registries | vtp}
no debug sw-vlan {badpmcookies | cfg-vlan  {bootup | cli} | events | ifs | mapping | notification | packets | redundancy | registries | vtp}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>badpmcookies</td>
<td>Displays debug messages for VLAN manager incidents of bad port manager cookies.</td>
</tr>
<tr>
<td>cfg-vlan</td>
<td>Displays VLAN configuration debug messages.</td>
</tr>
<tr>
<td>bootup</td>
<td>Displays messages when the switch is booting up.</td>
</tr>
<tr>
<td>cli</td>
<td>Displays messages when the command-line interface (CLI) is in VLAN configuration mode.</td>
</tr>
<tr>
<td>events</td>
<td>Displays debug messages for VLAN manager events.</td>
</tr>
<tr>
<td>ifs</td>
<td>Displays debug messages for the VLAN manager IOS file system (IFS). See debug sw-vlan ifs, on page 1558 for more information.</td>
</tr>
<tr>
<td>mapping</td>
<td>Displays debug messages for VLAN mapping.</td>
</tr>
<tr>
<td>notification</td>
<td>Displays debug messages for VLAN manager notifications. See debug sw-vlan notification, on page 1559 for more information.</td>
</tr>
<tr>
<td>packets</td>
<td>Displays debug messages for packet handling and encapsulation processes.</td>
</tr>
<tr>
<td>redundancy</td>
<td>Displays debug messages for VTP VLAN redundancy.</td>
</tr>
<tr>
<td>registries</td>
<td>Displays debug messages for VLAN manager registries.</td>
</tr>
<tr>
<td>vtp</td>
<td>Displays debug messages for the VLAN Trunking Protocol (VTP) code. See debug sw-vlan vtp, on page 1560 for more information.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The undebug sw-vlan command is the same as the no debug sw-vlan command.

This example shows how to display debug messages for VLAN manager events:

```
Device> enable
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `undebug sw-vlan ifs` command is the same as the `no debug sw-vlan ifs` command.

When selecting the file read operation, Operation 1 reads the file header, which contains the header verification word and the file version number. Operation 2 reads the main body of the file, which contains most of the domain and VLAN information. Operation 3 reads type length version (TLV) descriptor structures. Operation 4 reads TLV data.

This example shows how to display file-write operation debug messages:

```
Device> enable
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.

```
derbug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}

no debug sw-vlan notification {accfwdchange | allowedvlancfgchange | fwdchange | linkchange | modechange | pruningcfgchange | statechange}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accfwdchange</td>
<td>Displays debug messages for VLAN manager notification of aggregated access</td>
</tr>
<tr>
<td></td>
<td>interface spanning-tree forward changes.</td>
</tr>
<tr>
<td>allowedvlancfgchange</td>
<td>Displays debug messages for VLAN manager notification of changes to the</td>
</tr>
<tr>
<td></td>
<td>allowed VLAN configuration.</td>
</tr>
<tr>
<td>fwdchange</td>
<td>Displays debug messages for VLAN manager notification of spanning-tree</td>
</tr>
<tr>
<td></td>
<td>forwarding changes.</td>
</tr>
<tr>
<td>linkchange</td>
<td>Displays debug messages for VLAN manager notification of interface link-state</td>
</tr>
<tr>
<td></td>
<td>changes.</td>
</tr>
<tr>
<td>modechange</td>
<td>Displays debug messages for VLAN manager notification of interface mode</td>
</tr>
<tr>
<td></td>
<td>changes.</td>
</tr>
<tr>
<td>pruningcfgchange</td>
<td>Displays debug messages for VLAN manager notification of changes to the</td>
</tr>
<tr>
<td></td>
<td>pruning configuration.</td>
</tr>
<tr>
<td>statechange</td>
<td>Displays debug messages for VLAN manager notification of interface state</td>
</tr>
<tr>
<td></td>
<td>changes.</td>
</tr>
</tbody>
</table>

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `unddebug sw-vlan notification` command is the same as the `no debug sw-vlan notification` command.

This example shows how to display debug messages for VLAN manager notification of interface mode changes:

```
Device> enable
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.

**Syntax**

```
debug sw-vlan vtp  {events | packets | pruning  [ {packets | xmit}] | redundancy  | xmit}
no debug sw-vlan vtp  {events | packets | pruning | redundancy | xmit}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>events</strong></td>
<td>Displays debug messages for general-purpose logic flow and detailed VTP messages generated by the VTP_LOG_RUNTIME macro in the VTP code.</td>
</tr>
<tr>
<td><strong>packets</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>pruning</strong></td>
<td>Displays debug messages generated by the pruning segment of the VTP code.</td>
</tr>
<tr>
<td><strong>packets</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>xmit</strong></td>
<td>(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.</td>
</tr>
<tr>
<td><strong>redundancy</strong></td>
<td>Displays debug messages for VTP redundancy.</td>
</tr>
<tr>
<td><strong>xmit</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## 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.

This example shows how to display debug messages for VTP redundancy:
Device> enable
Device# debug sw-vlan vtp redundancy
**dot1q vlan native**

To assign the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic, use the `dot1q vlan native` command in interface configuration mode. To remove the VLAN ID assignment, use the `no` form of this command.

```markdown
**Syntax Description**

- `vlan-id`  Trunk interface ID. The range is from 1 to 4000.
- `native`  Specifies the native VLAN associated with the 802.1Q trunk interface.

**Command Default**

No default behavior or values

**Command Modes**

Interface configuration (config-if)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes proper task IDs. If you suspect that user group assignment is preventing you from using a command, contact your AAA administrator.

The `dot1q vlan native` command defines the default, or native VLAN, associated with an 802.1Q trunk interface. The native VLAN of a trunk interface is the VLAN to which all the untagged VLAN packets are logically assigned.

**Note**

The native VLAN cannot be configured on a subinterface of the trunk interface. The native VLAN must be configured with the same value at both ends of the link, or traffic can be lost or sent to the wrong VLAN.

The following example shows how to configure the native VLAN of a HundredGigabitEthernet 1/0/33 trunk interface as 1. Packets received on this interface that are untagged, or that have an 802.1Q tag with VLAN ID 1, are received on the main interface. Packets sent from the main interface are transmitted without an 802.1Q tag.

```sql
Device> enable
Device(config)# interface HundredGigabitEthernet 1/0/33.201
Device(config-subif)# dot1q vlan 1 native
```
interface (VLAN)

To create a VLAN subinterface, use the `interface` command in global configuration mode. To delete a subinterface, use the `no` form of this command.

```
interface {type switch |slot |port_subinterface }
no interface {type switch |slot |port_subinterface }
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>switch</code></td>
<td>Physical interfaces or virtual interfaces followed by the subinterface path ID.</td>
</tr>
<tr>
<td><code>slot</code></td>
<td>Physical interfaces or virtual interfaces followed by the subinterface path ID.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>Physical interfaces or virtual interfaces followed by the subinterface path ID.</td>
</tr>
<tr>
<td><code>subinterface</code></td>
<td>Physical interfaces or virtual interfaces followed by the subinterface path ID.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Gibraltar 16.10.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator.

To configure a large number of subinterfaces, we recommend entering all configuration data before you commit the interface command.

To change an interface from Layer 2 to Layer 3 mode and back, you must delete the interface first and then re-configure it in the appropriate mode.

This example shows how to configure subinterfaces on layer 3 interfaces:

```
Device> enable
Device(config)# interface HundredGigabitEthernet 1/0/33.201
Device(config-subif)# encapsulation dot1q 33 native
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1q vlan native</td>
<td>Defines the native VLAN ID associated with a subinterface.</td>
</tr>
</tbody>
</table>
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.
- **secondary-vlan-list**: 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>(Optional) Maps the secondary VLAN to the primary VLAN SVI.</td>
</tr>
<tr>
<td>remove</td>
<td>(Optional) Removes the mapping between the secondary VLAN and the primary</td>
</tr>
<tr>
<td></td>
<td>VLAN SVI.</td>
</tr>
<tr>
<td>secondary-vlan-list</td>
<td>One or more secondary VLANs to be mapped to the primary VLAN SVI.</td>
</tr>
</tbody>
</table>

**Command Default**

No private VLAN SVI mapping is configured.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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**

`interface-id` (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**
  - Cisco IOS XE Everest
  - 16.5.1a

- **Modification**
  - 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  301 community
vlan3 302  302 community
```

```
**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]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>(Optional) Displays one line for each VLAN with the VLAN name, status, and its ports.</td>
</tr>
<tr>
<td>dot1q tag native</td>
<td>(Optional) Displays the IEEE 802.1Q native VLAN tagging status.</td>
</tr>
<tr>
<td>group</td>
<td>(Optional) Displays information about VLAN groups.</td>
</tr>
<tr>
<td>id vlan-id</td>
<td>(Optional) Displays information about a single VLAN identified by the VLAN ID number. For <code>vlan-id</code>, the range is 1 to 4094.</td>
</tr>
<tr>
<td>mtu</td>
<td>(Optional) Displays a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN.</td>
</tr>
<tr>
<td>name vlan-name</td>
<td>(Optional) Displays information about a single VLAN identified by the VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.</td>
</tr>
<tr>
<td>private-vlan</td>
<td>(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.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Displays only private VLAN ID and type.</td>
</tr>
<tr>
<td>remote-span</td>
<td>(Optional) Displays information about Remote SPAN (RSPAN) VLANs.</td>
</tr>
<tr>
<td>summary</td>
<td>(Optional) Displays VLAN summary information.</td>
</tr>
</tbody>
</table>

**Note**

The `ifindex` keyword is not supported, even though it is visible in the command-line help string.

**Command Modes**

User EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
<th>Stp</th>
<th>BrdgMode</th>
<th>Trans1</th>
<th>Trans2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enet</td>
<td>100001</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>enet</td>
<td>100002</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>40</td>
<td>enet</td>
<td>100040</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>300</td>
<td>enet</td>
<td>100300</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1002</td>
<td>fddi</td>
<td>101002</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1003</td>
<td>tr</td>
<td>101003</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1004</td>
<td>fdnet</td>
<td>101004</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1005</td>
<td>trnet</td>
<td>101005</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2000</td>
<td>enet</td>
<td>102000</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3000</td>
<td>enet</td>
<td>103000</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 173: show vlan Command Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>VLAN number.</td>
</tr>
<tr>
<td>Name</td>
<td>Name, if configured, of the VLAN.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the VLAN (active or suspend).</td>
</tr>
<tr>
<td>Ports</td>
<td>Ports that belong to the VLAN.</td>
</tr>
<tr>
<td>Type</td>
<td>Media type of the VLAN.</td>
</tr>
<tr>
<td>SAID</td>
<td>Security association ID value for the VLAN.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit size for the VLAN.</td>
</tr>
<tr>
<td>Parent</td>
<td>Parent VLAN, if one exists.</td>
</tr>
<tr>
<td>RingNo</td>
<td>Ring number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>BrdgNo</td>
<td>Bridge number for the VLAN, if applicable.</td>
</tr>
<tr>
<td>Stp</td>
<td>Spanning Tree Protocol type used on the VLAN.</td>
</tr>
<tr>
<td>BrdgMode</td>
<td>Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB.</td>
</tr>
<tr>
<td>Trans1</td>
<td>Translation bridge 1.</td>
</tr>
<tr>
<td>Trans2</td>
<td>Translation bridge 2.</td>
</tr>
<tr>
<td>Remote SPAN VLANs</td>
<td>Identifies any RSPAN VLANs that have been configured.</td>
</tr>
<tr>
<td>Primary/Secondary/Type/Ports</td>
<td>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.</td>
</tr>
</tbody>
</table>

This is an example of output from the `show vlan dot1q tag native` command:

```
Device> enable
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
```
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 vtp

To display general information about the VLAN Trunking Protocol (VTP) management domain, status, and counters, use the `show vtp` command in EXEC mode.

```
show vtp [counters | devices [conflicts] | interface [interface-id] | password | status]
```

**Syntax Description**

- **counters**: Displays the VTP statistics for the device.
- **devices**: Displays information about all VTP version 3 devices in the domain. This keyword applies only if the device is not running VTP version 3.
- **conflicts**: (Optional) Displays information about VTP version 3 devices that have conflicting primary servers. This command is ignored when the device is in VTP transparent or VTP off mode.
- **interface**: Displays VTP status and configuration for all interfaces or the specified interface.
- **interface-id**: (Optional) Interface for which to display VTP status and configuration. This can be a physical interface or a port channel.
- **password**: Displays the configured VTP password (available in privileged EXEC mode only).
- **status**: Displays general information about the VTP management domain status.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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` 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` command did not specify the `hidden` keyword and encryption is enabled on the device, the encrypted password appears.
- If the `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> **enable**
Device# **show vtp devices**

Retrieving information from the VTP domain. Waiting for 5 seconds.

<table>
<thead>
<tr>
<th>VTP Database</th>
<th>Conf Device ID</th>
<th>Primary Server</th>
<th>Revision</th>
<th>System Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Yes</td>
<td>00b0.8e50.d000</td>
<td>000c.0412.6300 12354 main.cisco.com</td>
<td></td>
</tr>
<tr>
<td>MST</td>
<td>No</td>
<td>00b0.8e50.d000</td>
<td>0004.AB45.6000 24 main.cisco.com</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>Yes</td>
<td>000c.0412.6300-000c.0412.6300 67 qwerty.cisco.com</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:**

<table>
<thead>
<tr>
<th>Trunk</th>
<th>Join Transmitted</th>
<th>Join Received</th>
<th>Summary advts received from non-pruning-capable device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi1/0/47</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi1/0/48</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi2/0/1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Gi3/0/2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Table 174: show vtp counters Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary advertisements received</td>
<td>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.</td>
</tr>
<tr>
<td>Subset advertisements received</td>
<td>Number of subset advertisements received by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.</td>
</tr>
<tr>
<td>Request advertisements received</td>
<td>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.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Summary advertisements transmitted</td>
<td>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.</td>
</tr>
<tr>
<td>Subset advertisements transmitted</td>
<td>Number of subset advertisements sent by this device on its trunk ports. Subset advertisements contain all the information for one or more VLANs.</td>
</tr>
<tr>
<td>Request advertisements transmitted</td>
<td>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.</td>
</tr>
<tr>
<td>Number of configuration revision errors</td>
<td>Number of revision errors. Whenever you define a new VLAN, delete an existing one, suspend or resume an existing VLAN, or modify the parameters on an existing VLAN, the configuration revision number of the device increments. These revision errors increment whenever the device receives an advertisement whose revision number matches the revision number of the device, but the MD5 digest values do not match. This error means that the VTP password in the two devices is different or that the devices have different configurations. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</td>
</tr>
<tr>
<td>Number of configuration digest errors</td>
<td>Number of MD5 digest errors. Digest errors increment whenever the MD5 digest in the summary packet and the MD5 digest of the received advertisement calculated by the device do not match. This error usually means that the VTP password in the two devices is different. To solve this problem, make sure the VTP password on all devices is the same. These errors indicate that the device is filtering incoming advertisements, which causes the VTP database to become unsynchronized across the network.</td>
</tr>
</tbody>
</table>
Number of V1 summary 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
0xB9 0xB9 0x9B 0x70 0x03 0x61 0xE9 0x27
```

Table 175: show vtp status Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Version capable</td>
<td>Displays the VTP versions that are capable of operating on the device.</td>
</tr>
<tr>
<td>VTP Version running</td>
<td>Displays the VTP version operating on the device. By default, the device implements Version 1 but can be set to Version 2.</td>
</tr>
<tr>
<td>VTP Domain Name</td>
<td>Name that identifies the administrative domain for the device.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP Pruning Mode</td>
<td>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.</td>
</tr>
<tr>
<td>VTP Traps Generation</td>
<td>Displays whether VTP traps are sent to a network management station.</td>
</tr>
<tr>
<td>Device ID</td>
<td>Displays the MAC address of the local device.</td>
</tr>
<tr>
<td>Configuration last modified</td>
<td>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.</td>
</tr>
<tr>
<td>VTP Operating Mode</td>
<td>Displays the VTP operating mode, which can be server, client, or transparent.</td>
</tr>
<tr>
<td></td>
<td><strong>Server</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Client</strong> — 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Transparent</strong> — 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.</td>
</tr>
<tr>
<td>Maximum VLANs Supported Locally</td>
<td>Maximum number of VLANs supported locally.</td>
</tr>
<tr>
<td>Number of Existing VLANs</td>
<td>Number of existing VLANs.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------</td>
</tr>
<tr>
<td>Configuration Revision</td>
<td>Current configuration revision number on this device.</td>
</tr>
<tr>
<td>MD5 Digest</td>
<td>A 16-byte checksum of the VTP configuration.</td>
</tr>
</tbody>
</table>
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**: 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.

- **promiscuous**: 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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**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.

```bash
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.

```bash
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**
  - Sets the IP phone port to override the IEEE 802.1p priority received from the PC or the attached device with the specified class of service (CoS) value. The range is 0 to 7. Seven is the highest priority. The default is 0.

- **trust**
  - Sets the IP phone port to trust the IEEE 802.1p priority received from the PC or the attached device.

**Command Default**
The default port priority is set to a CoS value of 0 for untagged frames received on the port.

**Command Modes**
Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>16.5.1a</td>
<td></td>
</tr>
</tbody>
</table>

**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 the device access ports.

This example shows how to configure the IP phone connected to the specified port to trust the received IEEE 802.1p priority:

```
Device> enable
Device# configure terminal
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

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>allowed vlan vlan-list</code></td>
<td>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 <code>vlan-list</code> choices.</td>
</tr>
<tr>
<td><code>native vlan vlan-id</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>pruning vlan vlan-list</code></td>
<td>Sets the list of VLANs that are eligible for VTP pruning when in trunking mode. See the Usage Guidelines for the <code>vlan-list</code> choices.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### 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.

  - You can add extended-range VLANs to the allowed VLAN list, but not to the pruning-eligible VLAN list.

- **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.

Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
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> enable
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> enable
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> enable
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.
To add a VLAN and to enter the VLAN configuration mode, use the `vlan` command in global configuration mode. To delete the VLAN, use the `no` form of this command.

```
vlan vlan-id
no vlan vlan-id
```

**Syntax Description**
- `vlan-id` ID of the VLAN to be added and configured. The range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens.

**Command Default**
None

**Command Modes**
Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can use the `vlan ` global configuration command to add normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). Configuration information for normal-range VLANs is always saved in the VLAN database, and you can display this information by entering the `show vlan` privileged EXEC command. If the VTP mode is transparent, VLAN configuration information for normal-range VLANs is also saved in the device running configuration file. VLAN IDs in the extended range are not saved in the VLAN database, but they are stored in the switch running configuration file, and you can save the configuration in the startup configuration file.

VTP version 3 supports propagation of extended-range VLANs. VTP versions 1 and 2 propagate only VLANs 1 to 1005.

When you save the VLAN and VTP configurations in the startup configuration file and reboot the device, the configuration is selected as follows:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.
- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.

If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

Entering the `vlan` command with a VLAN ID enables VLAN configuration mode. When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit the VLAN configuration mode. Only the `shutdown` command (for VLANs 1 to 1005) takes effect immediately.
Although all commands are visible, the only VLAN configuration command that is supported on extended-range VLANs is `remote-span`. For extended-range VLANs, all other characteristics must remain at the default state.

These configuration commands are available in VLAN configuration mode. The `no` form of each command returns the characteristic to its default state:

- **are are-number** — Defines the maximum number of all-routes explorer (ARE) hops for this VLAN. This keyword applies only to TrCRF VLANs. The range is 0 to 13. The default is 7. If no value is entered, 0 is assumed to be the maximum.

- **backupcrf** — Specifies the backup CRF mode. This keyword applies only to TrCRF VLANs.
  - **enable** — Backup CRF mode for this VLAN.
  - **disable** — Backup CRF mode for this VLAN (the default).

- **bridge {bridge-number | type}** — Specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings that have this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0 (no source-routing bridge) for FDDI-NET, TrBRF, and Token Ring-NET VLANs. The `type` keyword applies only to TrCRF VLANs and is one of these:
  - **srb** — Source-route bridging
  - **srt** — Source-route transparent bridging

- **exit** — Applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.

- **media** — Defines the VLAN media type and is one of these:

  **Note** The device supports only Ethernet ports. You configure only FDDI and Token Ring media-specific characteristics for VLAN Trunking Protocol (VTP) global advertisements to other devices. These VLANs are locally suspended.

  - **ethernet** — Ethernet media type (the default).
  - **fd-net** — FDDI network entity title (NET) media type.
  - **fddi** — FDDI media type.
  - **tokenring** — Token Ring media type if the VTP v2 mode is disabled, or TrCRF if the VTP Version 2 (v) mode is enabled.
  - **tr-net** — Token Ring network entity title (NET) media type if the VTP v2 mode is disabled or TrBRF media type if the VTP v2 mode is enabled.

See the table that follows for valid commands and syntax for different media types.

- **name vlan-name** — Names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is VLANxxxx where xxxx represents four numeric digits (including leading zeros) equal to the VLAN ID number.
• **no**—Negates a command or returns it to the default setting.

• **parent parent-vlan-id**—Specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. This parameter identifies the TrBRF to which a TrCRF belongs and is required when defining a TrCRF. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN) for FDDI and Token Ring VLANs. For both Token Ring and TrCRF VLANs, the parent VLAN ID must already exist in the database and be associated with a Token Ring-NET or TrBRF VLAN.

• **remote-span**—Configures the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. If VTP is enabled, the new RSPAN VLAN is propagated by VTP for VLAN IDs that are lower than 1024. Learning is disabled on the VLAN.

• **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 176: Valid Commands and Syntax for Different Media Types**

<table>
<thead>
<tr>
<th>Media Type</th>
<th>Valid Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>name vlan-name, media ethernet, state {suspend</td>
</tr>
<tr>
<td>Media Type</td>
<td>Valid Syntax</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>FDDI</td>
<td>`name vlan-name, media fddi, state {suspend</td>
</tr>
<tr>
<td>FDDI-NET</td>
<td>`name vlan-name, media fd-net, state {suspend</td>
</tr>
<tr>
<td>If VTP v2 mode is disabled, do not set the stp type to auto.</td>
<td></td>
</tr>
<tr>
<td>Token Ring</td>
<td>VTP v1 mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>`name vlan-name, media tokenring, state {suspend</td>
</tr>
<tr>
<td>Token Ring concentrator relay function (TrCRF)</td>
<td>VTP v2 mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>`name vlan-name, media tokenring, state {suspend</td>
</tr>
<tr>
<td>Token Ring-NET</td>
<td>VTP v1 mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>`name vlan-name, media tr-net, state {suspend</td>
</tr>
<tr>
<td>Token Ring bridge relay function (TrBRF)</td>
<td>VTP v2 mode is enabled.</td>
</tr>
<tr>
<td></td>
<td>`name vlan-name, media tr-net, state {suspend</td>
</tr>
</tbody>
</table>

The following table describes the rules for configuring VLANs:
Table 177: VLAN Configuration Rules

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>VTP v2 mode is enabled, and you are configuring a TrCRF VLAN media type.</td>
<td>Specify a parent VLAN ID of a TrBRF that already exists in the database.</td>
</tr>
<tr>
<td></td>
<td>Specify a ring number. Do not leave this field blank.</td>
</tr>
<tr>
<td>VTP v2 mode is enabled, and you are configuring VLANs other than TrCRF media type.</td>
<td>Do not specify a backup CRF.</td>
</tr>
<tr>
<td>VTP v2 mode is enabled, and you are configuring a TrBRF VLAN media type.</td>
<td>Specify a bridge number. Do not leave this field blank.</td>
</tr>
<tr>
<td>VTP v1 mode is enabled.</td>
<td>No VLAN can have an STP type set to auto.</td>
</tr>
<tr>
<td></td>
<td>This rule applies to Ethernet, FDDI, FDDI-NET, Token Ring, and Token Ring-NET VLANs.</td>
</tr>
<tr>
<td>Add a VLAN that requires translational bridging (values are not set to zero).</td>
<td>The translational bridging VLAN IDs that are used must already exist in the database.</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td>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).</td>
</tr>
</tbody>
</table>

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a `vlan-name` of VLAN `xxxx`, where `xxxx` represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default media is ethernet; the state is active. The default said-value is 100000 plus the VLAN ID; the mtu-size variable is 1500; the stp-type is ieee. When you enter the `exit` VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does nothing.

This example shows how to create a new VLAN with all default characteristics and enter VLAN configuration mode:

```
Device(config)# vlan 200
Device(config-vlan)# exit
Device(config)#
```
This example shows how to create a new extended-range VLAN with all the default characteristics, to enter VLAN configuration mode, and to save the new VLAN in the device startup configuration file:

```
Device(config)# vlan 2000
Device(config-vlan)# end
Device# copy running-config startup config
```

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.

```plaintext
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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
When enabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are tagged.

When disabled, native VLAN packets going out of all IEEE 802.1Q trunk ports are not tagged.

For more information about IEEE 802.1Q tunneling, see the software configuration guide for this release.

This example shows how to enable IEEE 802.1Q tagging on native VLAN frames:

```
Device# configure terminal
Device (config)# vlan dot1q tag native
Device (config)# end
```

You can verify your settings by entering the `show vlan dot1q tag native` privileged EXEC command.
vtp (global configuration)

To set or modify the VLAN Trunking Protocol (VTP) configuration characteristics, use the vtp command in global configuration mode. To remove the settings or to return to the default settings, use the no form of this command.

```
vtp {domain  domain-name | file  filename | interface  interface-name [only] | mode  {client | off | server [transparent] [ {mst | unknown | vlan}] | password  password  [{hidden | secret}] | pruning | version number}}
no vtp {file | interface | mode  [{client | off | server | transparent}] [ {mst | unknown | vlan}] | password | pruning | version}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain</td>
<td>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.</td>
</tr>
<tr>
<td>domain-name</td>
<td></td>
</tr>
<tr>
<td>file</td>
<td>Specifies the Cisco IOS file system file where the VTP VLAN configuration is stored.</td>
</tr>
<tr>
<td>filename</td>
<td></td>
</tr>
<tr>
<td>interface</td>
<td>Specifies the name of the interface providing the VTP ID updated for this device.</td>
</tr>
<tr>
<td>interface-name</td>
<td></td>
</tr>
<tr>
<td>only</td>
<td>(Optional) Uses only the IP address of this interface as the VTP IP updater.</td>
</tr>
<tr>
<td>mode</td>
<td>Specifies the VTP device mode as client, server, or transparent.</td>
</tr>
<tr>
<td>client</td>
<td>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.</td>
</tr>
<tr>
<td>off</td>
<td>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.</td>
</tr>
<tr>
<td>server</td>
<td>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.</td>
</tr>
<tr>
<td>transparent</td>
<td>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.</td>
</tr>
<tr>
<td>mst</td>
<td>(Optional) Sets the mode for the multiple spanning tree (MST) VTP database (only VTP Version 3).</td>
</tr>
<tr>
<td>Keyword</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>unknown</td>
<td>(Optional) Sets the mode for unknown VTP databases (only VTP Version 3).</td>
</tr>
<tr>
<td>vlan</td>
<td>(Optional) Sets the mode for VLAN VTP databases. This is the default (only VTP Version 3).</td>
</tr>
<tr>
<td>password</td>
<td>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.</td>
</tr>
<tr>
<td>hidden</td>
<td>(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.</td>
</tr>
<tr>
<td>secret</td>
<td>(Optional) Allows the user to directly configure the password secret key (only VTP Version 3).</td>
</tr>
<tr>
<td>pruning</td>
<td>Enables VTP pruning on the device.</td>
</tr>
<tr>
<td>version number</td>
<td>Sets the VTP Version to Version 1, Version 2, or Version 3.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When you save VTP mode, domain name, and VLAN configurations in the device startup configuration file and reboot the device, the VTP and VLAN configurations are selected by these conditions:

- If the VTP mode is transparent in the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared), and the VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or domain name in the startup configuration do not match the VLAN database, the domain name and VTP mode and configuration for VLAN IDs 1 to 1005 use the VLAN database information.
The **vtp file** *filename* cannot be used to load a new database; it renames only the file in which the existing database is stored.

Follow these guidelines when configuring a VTP domain name:

- The device is in the no-management-domain state until you configure a domain name. While in the no-management-domain state, the device does not send any VTP advertisements even if changes occur to the local VLAN configuration. The device leaves the no-management-domain state after it receives the first VTP summary packet on any port that is trunking or after you configure a domain name by using the **vtp domain** command. If the device receives its domain from a summary packet, it resets its configuration revision number to 0. After the device leaves the no-management-domain state, it cannot be configured to reenter it until you clear the NVRAM and reload the software.

- Domain names are case-sensitive.

- After you configure a domain name, it cannot be removed. You can only reassign it to a different domain.

Follow these guidelines when setting VTP mode:

- The **no vtp mode** command returns the device to VTP server mode.

- The **vtp mode server** command is the same as **no vtp mode** except that it does not return an error if the device is not in client or transparent mode.

- If the receiving device is in client mode, the client device changes its configuration to duplicate the configuration of the server. If you have devices in client mode, be sure to make all VTP or VLAN configuration changes on a device in server mode, as it has a higher VTP configuration revision number. If the receiving device is in transparent mode, the device configuration is not changed.

- A device in transparent mode does not participate in VTP. If you make VTP or VLAN configuration changes on a device in transparent mode, the changes are not propagated to other devices in the network.

- If you change the VTP or VLAN configuration on a device that is in server mode, that change is propagated to all the devices in the same VTP domain.

- The **vtp mode transparent** command disables VTP from the domain but does not remove the domain from the device.

- In VTP Versions 1 and 2, the VTP mode must be transparent for VTP and VLAN information to be saved in the running configuration file.

- With VTP Versions 1 and 2, you cannot change the VTP mode to client or server if extended-range VLANs are configured on the switch. Changing the VTP mode is allowed with extended VLANs in VTP Version 3.

- The VTP mode must be transparent for you to add extended-range VLANs or for VTP and VLAN information to be saved in the running configuration file.

- VTP can be set to either server or client mode only when dynamic VLAN creation is disabled.

- The **vtp mode off** command sets the device to off. The **no vtp mode off** command resets the device to the VTP server mode.

Follow these guidelines when setting a VTP password:

- Passwords are case sensitive. Passwords should match on all devices in the same domain.

- When you use the **no vtp password** form of the command, the device returns to the no-password state.
• The **hidden** and **secret** keywords are supported only in VTP Version 3. If you convert from VTP Version 2 to VTP Version 3, you must remove the hidden or secret keyword before the conversion.

Follow these guidelines when setting VTP pruning:

• VTP pruning removes information about each pruning-eligible VLAN from VTP updates if there are no stations belonging to that VLAN.

• If you enable pruning on the VTP server, it is enabled for the entire management domain for VLAN IDs 1 to 1005.

• Only VLANs in the pruning-eligible list can be pruned.

• Pruning is supported with VTP Version 1 and Version 2.

Follow these guidelines when setting the VTP version:

• Toggling the Version 2 (v2) mode state modifies parameters of certain default VLANs.

• Each VTP device automatically detects the capabilities of all the other VTP devices. To use Version 2, all VTP devices in the network must support Version 2; otherwise, you must configure them to operate in VTP Version 1 mode.

• If all devices in a domain are VTP Version 2-capable, you only need to configure Version 2 on one device; the version number is then propagated to the other Version-2 capable devices in the VTP domain.

• If you are using VTP in a Token Ring environment, VTP Version 2 must be enabled.

• If you are configuring a Token Ring bridge relay function (TrBRF) or Token Ring concentrator relay function (TrCRF) VLAN media type, you must use Version 2.

• If you are configuring a Token Ring or Token Ring-NET VLAN media type, you must use Version 1.

• In VTP Version 3, all database VTP information is propagated across the VTP domain, not only VLAN database information.

• Two VTP Version 3 regions can only communicate over a VTP Version 1 or VTP Version 2 region in transparent mode.

You cannot save password, pruning, and version configurations in the device configuration file.

This example shows how to rename the filename for VTP configuration storage to vtpfilename:

```
Device(config)# vtp file vtpfilename
```

This example shows how to clear the device storage filename:

```
Device(config)# no vtp file vtpconfig
Clearing device storage filename.
```

This example shows how to specify the name of the interface providing the VTP updater ID for this device:

```
Device(config)# vtp interface gigabitethernet
```

This example shows how to set the administrative domain for the device:
Device(config)# vtp domain OurDomainName

This example shows how to place the device in VTP transparent mode:
Device(config)# vtp mode transparent

This example shows how to configure the VTP domain password:
Device(config)# vtp password ThisIsOurDomainsPassword

This example shows how to enable pruning in the VLAN database:
Device(config)# vtp pruning
Pruning switched ON

This example shows how to enable Version 2 mode in the VLAN database:
Device(config)# vtp version 2

You can verify your settings by entering the show vtp status privileged EXEC command.
vtp (interface configuration)

To enable the VLAN Trunking Protocol (VTP) on a per-port basis, use the `vtp` command in interface configuration mode. To disable VTP on the interface, use the `no` form of this command.

```
vtp
no vtp
```

**Syntax Description**

This command has no arguments or keywords.

**Command Modes**

Interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Enter this command only on interfaces that are in trunking mode.

This example shows how to enable VTP on an interface:

```
Device> enable
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**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mst</td>
<td>(Optional) Configures the device as the primary VTP server for the multiple spanning tree (MST) feature.</td>
</tr>
<tr>
<td>vlan</td>
<td>(Optional) Configures the device as the primary VTP server for VLANs.</td>
</tr>
<tr>
<td>force</td>
<td>(Optional) Configures the device to not check for conflicting devices when configuring the primary server.</td>
</tr>
</tbody>
</table>

**Command Default**

The device is a VTP secondary server.

**Command Modes**

Privileged EXEC

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**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> enable
Device# vtp primary vlan
Setting device to VTP TRANSPARENT mode.
```

You can verify your settings by entering the `show vtp status` privileged EXEC command.
vtp primary